MARYLAND DEPARTMENT OF TRANSPORTATION

Office of Procurement
TORFP: J028B8400024
SHA APPLICATION PORTFOLIO BUSINESS SERVICES
Addendum #1
April 11, 2018

Addendum #1 is being issued to provide Pre-Proposal Conference Information which includes the meeting agenda, sign-in sheet for the above-named TORFP. All information contained herein is binding on all offerors who respond to this TORFP.

SEE ATTACHED PRE-PROPOSAL INFORMATION:

1. **Meeting Agenda**
2. **Sign-in Sheets**

End of Addendum #1

Pre-Proposal Conference Procurement Review
TORFP: J02B8400024
SHA APPLICATION PORTFOLIO BUSINESS SERVICES

Wednesday, April 11, 2018 @ 10:00 a.m. (EST)

Welcome to the Pre-proposal conference for the Task Order Request For Proposals (TORFP) J01B8400024 for the SHA Application Portfolio Business Services. My name is Peggy Tischler and I am the Procurement Officer assigned to this TORFP.

If you have not already done so, please sign the attendance sheet and for those firms that are certified Minority Business Enterprise (MBE), Small Business Reserve (SBR) or Veteran-Owned Small Business Enterprise (VSBE) firms, please make note of that in the far right hand columns of the sign-in sheet.

In attendance with me today are Mark Harrison, SHA, who is the designated Contract Manager and also Vince Mise from the SHA Office of Traffic and Safety.

I will be going over the Procurement part of this project and will take any questions related to the procurement of this TORFP.

I will then turn the conference over to Mr. Harrison who will review the scope of work. We will do our best to answer all questions regarding the scope of work, but strongly suggest all questions requiring an official answer be submitted in writing.

No answers given at today's meeting will be considered binding or an amendment to the contract. Throughout this Pre-Proposal Conference, if you want a high-level response to any question you may have, I again ask that your questions be submitted to me, in writing via email.

Reminder to all Offerors:

- The main purpose of this pre-proposal conference is to review the procurement requirements, address concerns, provide clarification, and provide instructions pertaining to the solicitation and scope of work, and answer questions.

- This TORFP was released via email to all Master Contractors under Functional Area 1 on Wednesday, April 4, 2018.
- Offerors will have the opportunity to submit questions in writing; written **questions must be submitted to me at** ptischler@mdot.state.md.us The deadline for submission of questions is **Tuesday, April 17, 2018 at 2:00 pm (EST).**
- The Questions and Answers will be released via Addendum as soon as possible after the Question due date.
- Pre-proposal minutes, sign in sheet(s) and all questions and responses will be published as an addendum and become part of this solicitation.
- Changes to the scope of work or any response requirements will be published as an addendum and supersede the original published documents per COMAR 21.05.02.07.
- The due date and time for proposal Submission is **Monday, May 7, 2018 at 2:00 P.M. Local Time**. Please see Sections 1.1 and 5.4 for specific proposal submission information.
- As a reminder, the Technical Proposal submission along with all of the required Attachments (listed under Section 7 of the TORFP), are to be delivered together, but in a separate email from the Financial Proposal.
- BOTH THE TECHNICAL AND FINANCIAL PROPOSALS WILL NEED TO BE PASSWORD ENCRYPTED, WITH DIFFERENT PASSWORDS FOR EACH PROPOSAL TO (TECHNICAL AND FINANCIAL).
- Please submit your offer in the format listed in section 5.4 of the TORFP, as this will help to ensure that you have submitted all requested information as well as assist the evaluation team to determine that all information has been received.
- Please be sure to send your proposals early enough to allow sufficient time for your submission to arrive timely in the Procurement Officers inbox. "The date and time of an e-mail TORFP submission is determined by the date and time of arrival of all required files in the TO Procurement Officer's e-mail inbox."
- The State will award this project to One Master Contractor.
- You are required to provide the name/number of your point of contact to set up oral presentations or for correspondence.

- Please be sure to review Section 6.2 – Task Order Award Process.
- There is a 20% Minority Business Enterprise (MBE) Goal for this project. If there are any MDOT Certified MBE firms, or Veteran Owned Small Businesses in attendance today, this would be a good opportunity to network with Firms planning to submit as a Prime Contractor.

Friendly reminder:

- It is your responsibility to update your company's information/account as necessary in with DoIT. MDOT Procurement does not have the capability of updating contractor's information.
- Any questions or concerns regarding your DoIT account should be directed to DoIT
- Only the information communicated by the Procurement officer in writing shall be the official position of the MDOT. MDOT assumes no responsibility for information communicated by any other source.

MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF PROCUREMENT
TORFPJ02B8400024

TITLE: SHA APPLICATION PORTFOLIO BUSINESS SERVICES
DATE: Wednesday, April 11, 2018 at 10:00 am (EST) **[X] PRE PROPOSAL MEETING** **Page 1 of 5**

COMPANY NAME	PRINTED NAME	PHONE NUMBER	E-MAIL ADDRESS	MBE	SBR	VSBE
Dept. of Transportation	Joe Palechek	410-865-1137	jpalechek@mdot.state.md.us			
Dept. of Transportation	Peggy Tischler	410-865-2777	ptischler@mdot.state.md.us			
SNAP, Inc	Amit Arora	703-230-6631	aarora@snapinc.net	✓		
Serigor	Ashley Boykin	334.798.4420	ashley.boykin@serigor.com	✓		
SAIC	Eric Finkbeiner	804 481 1188	eric.j.finkbeiner			
PN Automation	Lawrence Pokroy	248-486-9011	LARRY@pnautomation.com	✓		
[redacted]						
iCube Systems	Narayan Athreya	703-272-3636	NVATHREYA@icubesys.com	✓	✓	
GANTECH	David Mullinix	410-507-5596	dmullinix@gantech.net	✓		
Group Z	Nora Presti	410 772 0888	npresti@group-z.net	✓	✓	
N-3 Technologies	NALINI BOURI	240-994-3188	nalini@n-3tech.com	✓	✓	
ITNova	James Black	443-906-6077	JBlack@ITNovaConsulting.com	✓	✓	
Stay Strong ←	ATTAIN	8026821190	SAshrafian@AHAin			
S-Techco	Sung Shaw	443-272-1580	Sung.shaw@Stechco.com	✓		
ITSI	Andrew Price	4434309014	aprice@itsi-inc.com	✓	✓	
3 Sigma Software	KRUSHANU MAJMUNDAR	443 681 7474	KRUSHANU@3SigmaSoftware.com	[redacted]		
ATLASTAR InfoSolutions	Theodore Williams II	410-730-4866	twilliams@atlastar.com	✓	✓	
COW	Randy Stapleton	301 525-4556	RANDSTA@COW.COM			

MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF PROCUREMENT
TORFPJ02B8400024

TITLE: SHA APPLICATION PORTFOLIO BUSINESS SERVICES
DATE: Wednesday, April 11, 2018 at 10:00 am (EST) **[X] PRE PROPOSAL MEETING**

COMPANY NAME	PRINTED NAME	PHONE NUMBER	E-MAIL ADDRESS	MBE	SBR	VSBE
Dept. of Transportation	Joe Palechek	410-865-1137	jpalechek@mdot.state.md.us			
Dept. of Transportation	Peggy Tischler	410-865-2777	ptischler@mdot.state.md.us			
DK Consulting, LLC	Erin Hamilton	443-552-5851	ehamilton@dkconsult.net	✓	✓	
Custom Software Systems	Robert Cusack	703-771-9757x2	RCusack@customsoftwaresystems.com		✓	
CNSI	Sameer Rawal	443-570-4959	SRAWAL@CNS-INC.COM			
CNSI	VIK MEHTA	240-481-3929	VIK.MEHTA@CNS-INC.COM			
Serv Beyond Solutions	Manu Bakshi	301-275-9983	MANU.BAKSHI@SERVBEYOND.COM			
Ohm Systems	PRAFUL PATEL	215 309-6233	PPatel@ohmsysinc.com	✓		
DEPT. OF TRANS.	CARL HUDEC	410-865-1372	chudec2@mdot.state.md.us			
CUSTOM SW SYSTEMS	DENN EDWARDS	410 507 8164	JEDWARDS@CUSTOMSOFTWARESYSTEMS.COM			
EDGEMARK	MIKE LABUS	301.580.7049	MLABUS@EDGEMARKFD.COM			
22nd CENTURY TECHNOLOGIES	REDDY BOLLINENI	502-488-0162	reddy.bollineni@tfcti.com			
ZDAAS LLC	Amjad Nagrah	443-995426	anagrah@zd-techsolutions.com			
CYQUENT, INC	SAGAR SAWANT	240-292-0234	ssawant@cyquent.com	✓	✓	

MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF PROCUREMENT
TORFPJ02B8400024

TITLE: SHA APPLICATION PORTFOLIO BUSINESS SERVICES
DATE: Wednesday, April 11, 2018 at 10:00 am (EST) **[X] PRE PROPOSAL MEETING**

COMPANY NAME	PRINTED NAME	PHONE NUMBER	E-MAIL ADDRESS	MBE	SBR	VSBE
Dept. of Transportation	Joe Palechek	410-865-1137	jpalechek@mdot.state.md.us			
Dept. of Transportation	Peggy Tischler	410-865-2777	ptischler@mdot.state.md.us			
ANGARAI	MONICA AHUJA	410-472-5000	MDBIDS@ANGARAI-INTL.COM	✓	✓	
ANGARAI	SHANKAR BALA	410-472-5000	"	✓	✓	
Three Sigma Software	ANJAN RENDEM	217-416-8631	anjan.rendem@3sigmaSoftware.com			
Intrusit	Munish Sahney	443 755 4556	Munish.Sahney@Intrusit.com	—		
Theresa Boyle	Theresa Boyle	443-542-9188	tboyle@apvit.com	✓	✓	
Christa Sklar	GANTECH	4104992881	cssklar@gantechnet	✓		
MDOT	Brenda Townsend-Milton	410-684-7055				
Dimensional Technical Services	Cindy Hill	301.370.3317	Cindyhill@dimensionaltek.com	✓	✓	

MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF PROCUREMENT
TORFPJ02B8400024

TITLE: SHA APPLICATION PORTFOLIO BUSINESS SERVICES
DATE: Wednesday, April 11, 2018 at 10:00 am (EST) **[X] PRE PROPOSAL MEETING**

COMPANY NAME	PRINTED NAME	PHONE NUMBER	E-MAIL ADDRESS	MBE	SBR	VSBE
Dept. of Transportation	Joe Palechek	410-865-1137	jpalechek@mdot.state.md.us			
Dept. of Transportation	Peggy Tischler	410-865-2777	ptischler@mdot.state.md.us			
SHA	MARK Harrison	410-454-865-	Mharrison3@sha.state.md.us			
GRDA	MANISH DAVE	703.277.7729	mdave@grda.com	✓	✓	
MDOT/TSO	Bryan Walker	410-865-1315	bwalker5@mdot.state.md.us			
MDOT/SHA	Vincent Mise	4107875843	vmise@mdot.state.md.us			
CALIBRE	MATT KILLMEYER	703 8718781	mkillmeyer@CALIBRESYS.COM			
DK consulting LLC.	Dana Kerr	443-552-5851	dkerr@dkconsult.net	✓	✓	

MARYLAND DEPARTMENT OF TRANSPORTATION
OFFICE OF PROCUREMENT
TORFPJ02B8400024

TITLE: SHA APPLICATION PORTFOLIO BUSINESS SERVICES
DATE: Wednesday, April 11, 2018 at 10:00 am (EST) **[X] PRE PROPOSAL MEETING** **Page 5 of 5**

COMPANY NAME	PRINTED NAME	PHONE NUMBER	E-MAIL ADDRESS	MBE	SBR	VSBE
Dept. of Transportation	Joe Palechek	410-865-1137	jpalechek@mdot.state.md.us			
Dept. of Transportation	Peggy Tischler	410-865-2777	ptischler@mdot.state.md.us			
~~Wordsworth Agency Inc~~						
Salem Info Tech Inc	Wordsworth Agency	703 731 9711	wagency aduraid@salem infotech.com			

MDOT
Rev. 04/14

CONSULTING AND TECHNICAL SERVICES+ (CATS+)

TASK ORDER REQUEST FOR PROPOSALS (TORFP)

MARYLAND DEPARTMENT OF TRANSPORTATION STATE HIGHWAY ADMINISTRATION (SHA)

SOLICITATION NUMBER J02B8400024

SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP

ISSUE DATE: APRIL 4, 2018

MARYLAND DEPARTMENT OF TRANSPORTATION STATE HIGHWAY ADMINISTRATION (SHA)

KEY INFORMATION SUMMARY SHEET

Solicitation Title:	**SHA APPLICATION PORTFOLIO BUSINESS SERVICES**
Solicitation Number (TORFP#):	**J02B8400024**
Functional Area:	**Functional Area #1 - Enterprise Service Provider (ESP)**
TORFP Issue Date:	Wednesday, April 4, 2018
TORFP Issuing Office:	Maryland Department of Transportation for the State Highway Administration (MDOT/SHA or the "Agency")
Agency Location:	SHA, 707 N. Calvert Street, Baltimore MD 21202
TO Procurement Officer: **e-mail:** **Office Phone:**	Peggy Tischler ptischler@mdot.state.md.us ptischler@mdot.state.md.us 410-865-2777
TO Manager: **e-mail:** **Office Phone:**	Mark W Harrison SHA Headquarters, Office of Information Technology, 707 N. Calvert St., Baltimore, MD 21202 Mharrison3@sha.state.md.us 410-545-8652
TO Proposals are to be sent to:	ptischler@mdot.state.md.us;
TO Pre-proposal Conference:	7201 Corporate Center Drive, Hanover MD 21076, 4th Floor Board Room Wednesday, 4/11/2018 at 10:00 AM – 11:30 AM (EST) See **Attachment 6** for directions.
TO Proposals Due (Closing) Date and Time:	Monday, 5/7/2018 at 2:00 PM (EST) Offerors are reminded that a completed Feedback Form is requested if a no-bid decision is made (see **Section 5**).
MBE Subcontracting Goal:	20% - with the following sub-goals: 7% for African-American MBEs, 2% for Hispanic-American MBEs, and 8% for Woman-Owned MBEs.
VSBE Subcontracting Goal:	0%
Task Order Type:	Time and Material with Fixed Price and Time and Material Work Orders

Task Order Duration:	Five (5) years, commencing on date of Notice-to-Proceed.
Primary Place of Performance:	Thirteen (13) initial TO Contractor resources located at: SHA Headquarters Office of Information Technology (OIT) 707 N. Calvert St., Baltimore, MD 21202 Five (5) initial TO Contractor resources located at: SHA Hanover Complex Office of Traffic and Safety 7491 Connelly Dr., Hanover, MD 21076
SBR Designation:	No
Federal Funding:	No
Questions Due Date and Time	Tuesday, 4/17/2018 at 2:00 PM (EST)

TABLE OF CONTENTS - TORFP

1 Minimum Qualifications

1.1 Offeror Personnel Minimum Qualifications

Only Offeror Key Personnel that meet the following minimum qualification criteria shall be eligible for consideration in the evaluation of this TORFP. (See Section 3.10.5 – Key Personnel Identified)

The Key personnel proposed under this TORFP and any proposed personnel in response to a Work Order must meet all minimum qualifications for the labor category proposed, as identified in the CATS+ RFP Section 2.10. Resumes shall clearly outline starting dates and ending dates for each applicable experience or skill. Refer to CATS+ RFP Section 2.10 for examples of duties and the required education, general and specialized experience for the Key Personnel.

Offeror must specify the labor category corresponding to the following position(s) listed below and on Attachment B - TO Financial Proposal Form:

1.1.1 Senior **.**Net Programmer

i. Six (6) years of professional experience working in the .Net Framework (all of: C#.net, ASP.net, and VB.net)

ii. Six (6) years of professional experience with all of: JavaScript programming, HTML, XML/XSL, and CSS

1.1.2 Senior SalesForce.com Programmer

i. Six (6) years of professional experience with VisualForce/APEX

ii. One (1) year of professional experience with Lightning Components

1.1.3 Senior PowerBuilder Programmer

i. Six (6) years of professional experience developing applications with PowerBuilder with at least one (1) year experience with PowerBuilder v12.6.

As proof of meeting experience requirements, references must be furnished that are able to attest to the Offeror Personnel Minimum Qualifications as well as meeting the identified labor category description as described in CATS+ RFP Section 2.10 (http://doit.maryland.gov/contracts/Documents/CATSPlus2016/060B2490023-2016CATSPlus2016RFP.pdf

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

2 TO Contractor Requirements: Scope of Work

2.1 Summary Statement

The Maryland Department of Transportation (MDOT) is issuing this CAT+ TORFP for the State Highway Administration (SHA or the "Agency") in order to augment the SHA OIT application support services with a minimum of eighteen (18) highly qualified technical programming resources in accordance with the scope of work described in this TORFP.

2.1.1 In addition to the initial four (4) resources who will be available as of NTP Date, SHA anticipates issuing a Work Order immediately upon Task Order award for fourteen (14) additional resources according to the Work Order Process in **Section 3.14**. SHA will have the option of adding up to two (2) additional resources to this Task Order for a maximum total of twenty (20) resources. All resources beyond the initial eighteen will be requested, as needed through a Work Order process (See **Section 3.14**). SHA intends to identify the NTP Date to establish an approximate 10 Business Day transition period with the incumbent provider, SHA intends NTP to be on or around December 10, 2018.

2.1.2 SHA intends to award this Task Order to one (1) Master Contractor that proposes a team of resources and a Staffing Plan that can best satisfy the Task Order requirements.

2.1.3 Master Contractors are advised that, should a solicitation or other competitive award be initiated as a result of activity or recommendations arising from this Task Order, the Offeror awarded this Task Order may not be eligible to compete if such activity constitutes assisting in the drafting of specifications, requirement, or design thereof.

2.1.4 A Task Order award does not assure a TO Contractor that it will receive all Agency business under the Task Order.

2.2 Background and Purpose

The SHA is responsible for all interstates, U.S. and Maryland numbered routes excluding those in Baltimore City and toll facility maintained highways. The State system includes approximately 6,000 centerline miles, (16,064 lane miles) of highways and 2,400 bridges, connecting all regions of the State.

The SHA Business overview is available online at: www.roads.maryland.gov.

The SHA Office of Information Technology (OIT) application services section provides application support to its user base as follows:

A. Production issues: this is priority one and addresses any issues with a live production version of an application that hinders or prevents users from performing their duties, or that has a negative impact on the organization.

B. Enhancements to existing production versions: this requires new code to add enhanced features or capabilities to an existing application.

C. New applications: more in-depth functionality, and closely tied to the Advertising Schedule.

There will be occasions where programmers shall share the responsibility in addressing application bugs and new application enhancements as well as the development of other new project assignments based on workload and demand. **It is our expectation to acquire a TO Contractor who can provide programmers who are multi-skilled in the various programming languages as outlined in sections 1.1 Offeror Personnel Minimum Qualifications and section 2.3 Responsibilities and Tasks.**

There are currently two separate development groups, one located in Hanover, MD at: 7491 Connelly Drive, Hanover MD 21076 and the other in downtown Baltimore at: 707 N. Calvert street, Baltimore MD 21202.

2.2.1 Existing Software

A. Maximo is used as the SHA Help Desk tool to record, manage and report on service requests

B. Team Foundation Server is used for configuration and change management

2.2.2 State Staff and Roles

In addition to the TO Manager, the TO Contractor Personnel should expect to interact with other SHA personnel and contractors to meet the Agency's needs. Roles that will be working closely with the TO Contractor Personnel include, but are not limited to:

A. Business Analyst (this is typically a contractor)

The Business Analyst (BA) is responsible for analyzing the business process associated with each project request. The BA will produce detailed requirements that the programmer will use to develop code relevant to the application request.

B. Project Manager (this could be a SHA employee or a contractor)

The Project Manager (PM) is responsible for the facilitation and integration of efforts that are part of the project solution. The PM will work closely with the programmer and the customer. The PM is a certified Project Management Professional (PMP) that utilizes the methodologies as described in the Project Managers Book of Knowledge (PMBOK), part of the Project Management Institute (PMI).

C. Document Specialist (this is typically a contractor)

The Documentation Specialist (DS) is responsible for assisting in the development of the project references in association with the programmer. These references include the technical guide, user guide, and other references as needed.

D. Database Administrator (this is typically a contractor)

The Database Administrator (DBA) is responsible for data centric efforts related to a project. Some of the common efforts that the DBA and programmer will be involved in deal with data integration and properly mapping values to a project's data repository, and reviewing data for security sensitivity, such as Personally Identifiable Information (PII).

E. Web Services (this could be a SHA employee or a contractor)

The Web Services group will work closely with the programmer to deploy web based applications. The collaboration involves identifying the technical information needed to deploy to production, rollback plans, and customer contact information.

F. Network Administrator (this could be a SHA employee or a contractor)

The Network Administrator will be available to work with the programmer in establishing new network connectivity as well as any production issues with current connectivity.

G. Customers (typically a SHA employee)

The programmer will be involved with Joint Application Design (JAD) sessions with the customer and project team. There will be times when the programmer will need to work closely with the customer to gain a deeper understanding of project requirements and customer concerns.

H. Application Support Manager (typically a SHA employee)

The programmer will report to the Application Support Manager (ASM). The ASM will assign work to the programmer, review the programmer's weekly activity, and manager any conflicts the programmer may encounter.

2.2.3 Other State Responsibilities

A. The State will provide normal office working facilities and equipment reasonably necessary for TO Contractor performance under this Task Order. Any special requirements (e.g., reprographic services, computer time, key data entry) shall be identified.

B. The State is responsible for providing required information, data, documentation, and test data to facilitate the TO Contractor's performance of the work, and will provide such additional assistance and services as is specifically set forth.

2.3 Responsibilities and Tasks

2.3.1 General Responsibilities

A. TO Contractor Personnel shall provide technical expertise and advice to SHA staff and management.

B. TO Contractor Personnel shall assist the PM and BA in the preparation of documentation to describe new or changed processes.

C. TO Contractor Personnel shall respond to information requests that business users submit through SHA's Maximo Automated Help Desk Application (Maximo) or the Office of Traffic and Safety (OOTS) IT Help Desk.

D. TO Contractor Personnel shall respond to trouble reports or change requests (TR / CR Log) reported through Maximo or the OOTS IT Help Desk.

E. TO Contractor Personnel shall assist in research and recommendations on new technologies.

F. TO Contractor Personnel shall assist in the development of Microsoft Software Storage Client (MSSC) objects used to implement and upgrade client software.

G. TO Contractor Personnel shall assist in the preparation and implementation of disaster recovery plans for various systems. TO Contractor Personnel shall create upgrade and migration schedules with plans that will minimize the impact on production and mission critical systems.

H. TO Contractor Personnel shall train end users on assigned applications, as needed.

I. TO Contractor Personnel shall attend organizational meetings as directed.

2.3.2 Existing System Maintenance Responsibilities

A. TO Contractor Personnel shall provide ongoing support for various SHA applications and technologies, as assigned.

B. TO Contractor Personnel shall maintain a TR and CR Log for each assigned application using Team Foundation Server or SharePoint environments, as directed.

C. TO Contractor Personnel shall remediate application defects reported through Maximo, OOTS IT Help Desk or from the business side System Administrators.

D. TO Contractor Personnel shall evaluate, design, and code approved application CRs.

E. TO Contractor Personnel shall perform integration testing any code and configuration changes prior to releasing for User Acceptance Testing (UAT).

F. TO Contractor Personnel shall maintain configuration and version control using Team Foundation Server.

G. TO Contractor Personnel shall assist in the development of application maintenance plans for scheduled maintenance activities.

H. TO Contractor Personnel shall recommend and assist in the development and implementation of maintenance plans for system upgrades and technology refreshes.

I. TO Contractor Personnel shall, in conjunction with the PM and BA, maintain and update System Documentation including but not limited to:

1. Interface Control Documents
2. User Guides
3. Administrator Guides
4. Test Cases
5. Release Notes
6. Security Procedures

J. TO Contractor Personnel shall develop system source code and executables using, but not limited to, the following primary technologies:

1. Microsoft Access 2007 or later version
2. C#.NET,
3. VB.NET,
4. SalesForce.com VisualForce/APEX, Lightning components
5. PowerBuilder v12.6,
6. Visual Basic 6.0,
7. ASP.NET
8. ASP 3.0
9. Delphi

2.3.3 New System Development Responsibilities

A. TO Contractor Personnel shall assist the PM in the gathering and development of system requirements.

B. TO Contractor Personnel shall analyze, recommend and design appropriate system security according to policies for data and application security using MDOT and DoIT's security standards.

C. TO Contractor Personnel shall recommend system design and participate in design revision reviews.

D. TO Contractor Personnel shall design the data model used by the application.

E. TO Contractor Personnel shall develop system source code and executables using, but not limited to, one of the following primary technologies:

1. Microsoft Access 2007 or later version
2. C#.NET,
3. ASP.NET,
4. VB.NET,
5. SalesForce.com VisualForce/APEX
6. SalesForce1 and Lightning components
7. PowerBuilder v12.6 or later version

F. TO Contractor Personnel shall maintain Configuration and Version Control using Team Foundation Server.

G. TO Contractor Personnel shall, in conjunction with the PM and BA, prepare repeatable test plans for rigorous testing of database servers and application upgrades.

H. TO Contractor Personnel shall perform unit, integration, and system testing.

I. TO Contractor Personnel shall maintain Test Problem Report through the use of Team Foundation Server or SharePoint environments.

J. TO Contractor Personnel shall assist with the installation and implementation of Agency-approved new application system software.

K. TO Contractor Personnel shall, in conjunction with the PM and BA, assist with the development of System Documentation including but not limited to:

1. Design Document
2. Interface Control Documents
3. Source Code Documents
4. Test Data and Test Cases
5. Test Reports with Results
6. Users Guides
7. Administrator Guides
8. Implementation Plan
9. Release Notes
10. Security Procedures

L. TO Contractor Personnel shall maintain a TR / CR Log for new application through the use of Team Foundation Server or SharePoint environments.

2.3.4 Non-Functional, Non-Technical Requirements

A. TO Contractor Personnel shall be responsible for knowledge transfer, occurring on the reassignment of a project resource from one task/project to another (either permanent or temporary transfer).

B. TO Contractor Personnel shall complete SHA-mandated core training prior to arrival to assigned SHA facilities

1. Each TO Contractor resource assigned to work on-site at an SHA facility and or SHA project site for a period of three (3) months or longer, regardless of the number of days worked per week, shall be required to take the following four (4) MANDATORY TRAINING COURSES given to all SHA employees and on-site TO Contractors:

a) ADA Awareness

b) Limited English Proficiency

c) Sexual Harassment Awareness

d) Workplace and Domestic Violence Awareness

2. This MANDATORY TRAINING shall be completed prior to the on-site TO Contractor resource's start date at the SHA facility (and/or project site). **Failure to complete this training prior to the resources start date could be grounds for termination.**

3. Each on-site TO Contractor resource shall provide certification of training completion by printing the certificate of completion available at the end of each training course and furnishing the printed copy to the TO Manager as record of completion

4. The on-site TO Contractor resource shall also forward a copy of all training certificates to the TO Contractor for its contract management records.

5. The TO Contractor cannot bill the hours required for its resources to complete this MANDATORY TRAINING. The hours estimated to complete all four (4) training courses is approximately 8 hours and will be available on-line from SHA's Internet Web site. There will be no cost for materials or the training course itself.

C. TO Contractor Personnel shall participate in meetings as a technical resource, as required.

D. TO Contractor Personnel shall support annual SHA initiatives involving technology of applications, such as the annual SHA online employee survey.

E. TO Contractor Personnel shall be responsible for reviewing technical documentation that may be authored by other resources for correctness.

F. TO Contractor Personnel shall, in conjunction with the PM, conduct training for end users, as necessary.

G. TO Contractor Personnel shall maintain workstations, including cleaning and reinstalling after a re-image.

H. TO Contractor Personnel shall perform product assessment of new technology as directed by the Agency.

I. TO Contractor Personnel shall attend technology or skill training, as required, at no cost to the Agency, to include, but not be limited to training that ensures TO Contractor Personnel (see Section 3.10.11):

1. To be competent in the practical use of new versions of existing SHA technologies,

2. To be competent in the practical use of new SHA technologies, and

3. To elevate competency with existing SHA technologies.

J. TO Contractor Personnel shall enter information into OIT's portfolio management software (Innotas) including status updates and time spent on projects.

2.3.5 Required Project Policies, Guidelines and Methodologies

The TO Contractor shall be required to comply with all applicable laws, regulations, policies, standards and guidelines affecting Information Technology projects, which may be created or changed periodically. Offeror is required to review all applicable links provided below and state compliance in its response.

It is the responsibility of the TO Contractor to ensure adherence and to remain abreast of new or revised laws, regulations, policies, standards and guidelines affecting project execution. These include, but are not limited to:

A. The State of Maryland System Development Life Cycle (SDLC) methodology at: www.DoIT.maryland.gov - keyword: SDLC;

B. The State of Maryland Information Technology Security Policy and Standards at: www.DoIT.maryland.gov - keyword: Security Policy;

C. The State of Maryland Information Technology Non-Visual Standards at: http://doit.maryland.gov/policies/Pages/ContractPolicies.aspx;

D. The State of Maryland Information Technology Project Oversight at: http://doit.maryland.gov/epmo/Pages/MITDP/oversight.aspx;

E. The TO Contractor shall follow project management methodologies consistent with the most recent edition of the Project Management Institute's *Project Management Body of Knowledge Guide*; and

F. TO Contractor Personnel shall follow a consistent methodology for all Task Order activities.

G. MDOT Information Security Plan (See Appendix 5)

H. MDOT ITIL Procedures and Practices as approved and implemented by MDOT.

2.3.6 Staffing Plan

Offerors shall describe in a Staffing Plan how all of the following additional resources, those other than the four (4) Key resources, shall be acquired to meet the needs of the Agency. Each job role below may be paired with a single CATS+ labor category. See Section 2.10 of the CATS+ Master Contract.

A. Eight (8) additional .Net Programmers
Each .Net Programmer is expected to possess the following experience:
   i. Four (4) years of professional experience working in the .Net Framework (C#.net, ASP.net or VB.net)
   ii. Four (4) years of professional experience with JavaScript programming, HTML, XML/XSL, and CSS

B. Two (2) additional Senior .Net Programmers
Each Senior .Net Programmer is expected to possess the following experience:
   i. Six (6) years of professional experience working in the .Net Framework (C#.net, ASP.net or VB.net)
   ii. Six (6) years of professional working experience with JavaScript programming, HTML, XML/XSL, and CSS

C. Two (2) additional SalesForce.com Programmers
Each SalesForce.com Programmer is expected to possess the following experience:
i. Four (4) years of professional experience with VisualForce/APEX
ii. One (1) year of professional experience with Lightning Components

D. One (1) additional Senior SalesForce.com Programmer
Each Senior SalesForce.com Programmer is expected to possess the following experience:
i. Six (6) years of professional working experience with VisualForce/APEX
ii. One (1) year of professional working experience with Lightning Components

E. One (1) additional PowerBuilder Programmer
Each PowerBuilder Programmer is expected to possess the following experience:
i. Four (4) years of professional experience developing applications with PowerBuilder with at least one (1) year experience with PowerBuilder v12.6

2.4 Deliverables

2.4.1 Deliverable Descriptions/Acceptance Criteria

A. TO Contractor Personnel shall produce, contribute to, and revise work products and deliverables as directed by the Agency.

B. TO Contractor Personnel shall recommend work products and deliverables for best execution of the Agency's needs.

ID #	Deliverable Description	Acceptance Criteria	Due Date / Frequency
1	Weekly TO Contractor Personnel Status Reports	Microsoft Word template (see Appendix 6) that contains the following: a. Activities completed with hours of effort, b. Activities in progress with hours of effort, c. Next weeks planned activities, d. Activities on hold/issues, e. Activities requiring overtime with hours of effort, f. Action items	Weekly TO Contractor Personnel Status Report emailed to the Application Services Manager by Friday Close of Business (COB)
2	Minority Business Enterprise (MBE) Report	See Section 3.12	See Section 3.12
3	TORFP progress, budget and MBE review session	A meeting with the TO Manager and OIT leadership to review progress on the TORFP including budget and the MBE goal.	Yearly to fall within 2 weeks of the anniversary of the NTP.

2.5 Optional Features, Future Work

2.5.1 Change Orders

A. If the TO Contractor is required to perform work beyond the scope of this TORFP, or there is a work reduction due to unforeseen scope changes, a TO Change Order is required. The TO Contractor and TO Manager shall negotiate a mutually acceptable price modification based on the TO Contractor's proposed rates in the Master Contract and scope of the work change.

B. No scope of work changes shall be performed until a change order is approved by DoIT and executed by the TO Procurement Officer.

2.6 Service Level Agreement (SLA)

THIS SECTION IS NOT APPLICABLE TO THIS TORFP.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

3 TO Contractor Requirements: General

3.1 Task Order Initiation Requirements

A. TO Contractor shall schedule and hold a kickoff meeting within 10 Business Days after NTP Date. At the kickoff, the TO Contractor shall furnish/review:

1. The Staffing Plan execution
   i. Time table for resume review
   ii. Time table for interviews
   iii. Time table for on-boarding
2. The plan for transition
   i. Application knowledge transfer
   ii. Toolset knowledge transfer
   iii. Standard Operating Procedures
   iv. Best practices utilized
3. Any questions that need clarification

B. Individual TO Contractor Personnel shall complete the mandatory training prior to presenting themselves for Agency on-site work. See **2.3.4.B.**

3.2 End of Task Order Transition

3.2.1 The TO Contractor shall provide transition assistance as requested by the State to facilitate the orderly transfer of services to the State or a follow-on contractor, for a period up to 30 working days prior to Task Order end date, or the termination thereof. Such transition efforts shall consist, not by way of limitation, of:

A. Provide additional services and/or support as requested to successfully complete the transition;

B. Maintain the services called for by the Task Order at the required level of proficiency;

C. Provide updated System Documentation, as appropriate; and

D. Provide current operating procedures (as appropriate).

3.2.2 The TO Contractor shall work toward a prompt and timely transition, proceeding in accordance with the directions of the TO Manager. The TO Manager may provide the TO Contractor with additional instructions to meet specific transition requirements prior to the end of Task Order.

3.2.3 The TO Contractor shall ensure that all necessary knowledge and materials for the tasks completed are transferred to the custody of State personnel or a third party, as directed by the TO Manager.

3.2.4 The TO Contractor shall support end-of-Task Order transition efforts with technical and project support to include but not be limited to:

A. The TO Contractor shall provide a draft Transition-Out Plan 120 Business Days in advance of Task Order end date.

B. The Transition-Out Plan shall address at a minimum the following areas:

1. Any staffing concerns/issues related to the closeout of the Task Order;
2. Communications and reporting process between the TO Contractor, the Agency and the TO Manager;
3. Security and system access review and closeout;
4. Any hardware/software inventory or licensing including transfer of any point of contact for required software licenses to the Agency or a designee;
5. Any final training/orientation of Agency staff;
6. Connectivity services provided, activities and approximate timelines required for Transition-Out;
7. Knowledge transfer, to include:
   a) A working knowledge of the current system environments as well as the general business practices of the Agency;
   b) Review with the Agency the procedures and practices that support the business process and current system environments;
   c) Working knowledge of all technical and functional matters associated with the Solution, its architecture, data file structure, interfaces, any batch programs, and any hardware or software tools utilized in the performance of this Task Order;
   d) Documentation that lists and describes all hardware and software tools utilized in the performance of this Task Order;
   e) A working knowledge of various utilities and corollary software products used in support and operation of the Solution;
8. Plans to complete tasks and any unfinished work items (including open change requests, and known bug/issues); and
9. Any risk factors with the timing and the Transition-Out schedule and transition process. The TO Contractor shall document any risk factors and suggested solutions.

C. The TO Contractor shall ensure all documentation and data including, but not limited to, System Documentation and current operating procedures, is current and complete with a hard and soft copy in a format prescribed by the TO Manager.

D. The TO Contractor shall provide copies of any current daily and weekly back-ups to the Agency or a third party as directed by the TO Manager as of the final date of transition, but no later than the final date of the Task Order.

E. Access to any data or configurations of the furnished product and/or services shall be available after the expiration of the Task **Order.**

3.2.5 Return and Maintenance of State Data

This section does not apply

3.3 Invoicing

3.3.1 Definitions

A. "Proper Invoice" means a bill, written document, or electronic transmission, readable by the agency, provided by a vendor requesting an amount that is due and payable by law under a written

procurement contract for property received or services rendered that meets the requirements of COMAR 21.06.09.02.

B. "Late Payment" means any amount that is due and payable by law under a written procurement contract, without deferral, delay, or set-off under COMAR 21.02.07.03, and remains unpaid more than 45 days after an agency receives a Proper Invoice.

C. "Payment" includes all required processing and authorization by the Comptroller of the Treasury, as provided under COMAR 21.02.07, and may be deferred, delayed, or set-off as applicable under COMAR 21.02.07.03.

3.3.2 General

A. Invoice payments to the TO Contractor shall be governed by the terms and conditions defined in the CATS+ Master Contract.

B. Any on-call hours and upgrades performed during non-Business Hours shall be billed based on actual time worked at the approved Task Order labor rates.

C. The TO Contractor shall send the original of each invoice and supporting documentation (itemized billing reference for employees, including detail of work) to:

1) E-Mail: sha-oit-invoice@sha.state.md.us for OIT assigned resources

2) E-Mail: Office of Traffic and Safety, point of contact will be named after award

3) The TO Manager's name must be shown on the E-mail Subject Line

D. Invoices for final payment shall be clearly marked as "FINAL" and submitted when all work requirements have been completed and no further charges are to be incurred under the TO Agreement. In no event shall any invoice be submitted later than 60 calendar days from the TO Agreement termination date.

E. Invoices submitted without the required information cannot be processed for payment. Payment of invoices may be withheld if any required documentation is not submitted including without limitation status reports. A Proper Invoice, required as Payment documentation, must include the following information, without error:

1. TO Contractor name and address;
2. TO Contractor point-of-contact with telephone number;
3. Remittance address;
4. Federal taxpayer identification (FEIN) number, social security number, as appropriate;
5. Invoice period (i.e. time period during which services covered by invoice were performed);
6. Invoice date;
7. Invoice number;
8. State assigned TO Agreement number and Title;
9. SHA issued (Blanket) Purchase Order number(s);
10. Labor Category;
11. Services provided broken down by specific resource to include Labor Category and quantity.

12. Amount due; and
13. Award amount;
14. Amount billed to date;
15. Amount remaining on contract;
16. MBE award amount;
17. MBE amount billed to date;
18. MBE percentage committed;
19. Any additional documentation required by regulation or the Task Order.

3.3.3 Invoice Submission Schedule

The TO Contractor shall submit monthly invoices for SHA approval and payment that coincide with the submission of the Weekly TO Contractor Personnel Status Reports for the month on or before the 10th day of the month. The invoices shall identify actual hours by each person assigned to the Task Order during the reporting period. Invoices shall be accompanied by timesheets documenting charges for labor in accordance with the TO Financial Proposal.

Invoices and all required documentation shall reflect the first day of the month through the last day of the month, **only**. Any piece of documentation showing hours worked the days before or after any given documented month will be incorrect and the TO Contractor shall be required to resubmit the entire package. Any documentation received after the 10th day of any month will be considered late. If the 10th of any month falls on a weekend, government holiday, or State of Maryland Service Reduction day, all documentation is due the last government Business Day prior.

It shall be the sole responsibility of the TO Contractor to ensure that all required monthly documentation is received by the 10th of each month.

3.3.4 For the purposes of this Task Order an amount will not be deemed due and payable if:

A. The amount invoiced is inconsistent with the Task Order.

B. The proper invoice has not been received by the party or office specified in the Task Order.

C. The invoice or performance is in dispute or the TO Contractor has failed to otherwise comply with the provisions of the Task Order.

D. The item or services have not been accepted.

E. The quantity of items delivered is less than the quantity ordered.

F. The items or services do not meet the quality requirements of the Task Order

G. If the Task Order provides for progress payments, the proper invoice for the progress payment has not been submitted pursuant to the schedule.

H. The TO Contractor has not submitted satisfactory documentation or other evidence reasonably required by the TO Procurement Officer or by the contract concerning performance under the contract and compliance with its provisions.

3.3.5 Travel Reimbursement

A. There shall be no reimbursement for Routine Travel. TO Contractor shall not be reimbursed for Non-Routine Travel without prior TO Manager approval.

B. Routine Travel is defined as travel within a 50-mile radius of the Agency's base location, as identified in the TORFP, or the TO Contractor's facility, whichever is closer to the consulting site. There will be no payment for labor hours for travel time or reimbursement for any travel expenses for work performed within these radiuses or at the TO Contractor's facility.

C. Non-routine Travel is defined as travel beyond the 50-mile radius of Agency's base location, as identified in the TORFP, or the TO Contractor's facility, whichever is closer to the consulting site. Non-routine travel will be identified within a TO Agreement, if appropriate, and will be reimbursed according to the State's travel regulations and reimbursement rates, which can be found at: www.DBM.maryland.gov - search: Fleet Management. If non-routine travel is conducted by automobile, the first 50 miles of such travel will be treated as routine travel and as described in **Section 3.3.7.A**, and will not be reimbursed. The TO Contractor may bill for labor hours expended in non-routine traveling beyond the identified 50-mile radius, only if so specified in the TORFP or Work Order.

3.3.6 Retainage

This section does not apply to this TORFP.

3.4 Liquidated Damages

MBE Liquidated damages are identified in **Attachment M**.

This solicitation does not require additional liquidated damages.

3.5 Disaster Recovery and Data

The following requirements apply to the TO Agreement:

3.5.1 Redundancy, Data Backup and Disaster Recovery

A. Resources shall be required to support SHA disaster recovery according to SHA's Disaster Recovery Plan and as assigned by SHA.

B. The SHA outlines its complete application restoration strategy for each application in its Disaster Recovery Plan. The developer portion of the disaster recovery plan for each application can be roughly summarized as follows (with the assumption that any hardware asset recovery has already been completed by OIT's Network & Desktop support group):

1. Attempt to restore the application installation directly from the Business Day Backup archive
2. If Step 1 is not feasible, retrieve the source code from Team Foundation Server and reinstall/configure the application manually.
3. In either case, once the application has been re-implemented / restored, the programmer reconnects the application to its data center, either its normal data center, or one restored from Business Day Backups by the Database Administration section.
4. Any additional modules or connections required for normal operation are re-implemented / restored.
5. The programmer tests the application for correctness and declares it ready for operational use if no further corrective action is required.

3.5.2 Data Ownership and Access

A. Data, databases and derived data products created, collected, manipulated, or directly purchased as part of a TORFP shall become the property of the State. The purchasing State agency is considered the custodian of the data and shall determine the use, access, distribution and other conditions based on appropriate State statutes and regulations.

B. Public jurisdiction user accounts and public jurisdiction data shall not be accessed, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of the Task Order, including as necessary to perform the services hereunder or (4) at the State's written request.

C. The TO Contractor shall limit access to and possession of State data to only TO Contractor Personnel whose responsibilities reasonably require such access or possession and shall train such TO Contractor Personnel on the confidentiality obligations set forth herein.

D. At no time shall any data or processes – that either belong to or are intended for the use of the State or its officers, agents or employees – be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

E. The Contractor shall not use any information collected in connection with the services furnished under this Contract for any purpose other than fulfilling such services.

3.5.3 Provisions in Sections 3.5.1 – 3.5.2 shall survive expiration or termination of the TO Agreement. Additionally, the TO Contractor and shall flow down the provisions of Sections 3.5.1-3.5.2 (or the substance thereof) in all subcontracts.

3.6 Insurance Requirements

3.6.1 Offeror shall confirm that, as of the date of its proposal, the insurance policies incorporated into its Master Contract are still current and effective at the required levels (See Master Contract Section 2.7).

3.6.2 The Offeror shall also confirm that any insurance policies intended to satisfy the requirements of this TORFP are issued by a company that is licensed to do business in the State of Maryland.

3.7 Security Requirements

3.7.1 Employee Identification

A. TO Contractor Personnel shall display his or her company ID badge in a visible location at all times while on State premises. Upon request of authorized State personnel, each such TO Contractor Personnel shall provide additional photo identification.

B. TO Contractor Personnel shall cooperate with State site requirements, including but not limited to, being prepared to be escorted at all times, and providing information for State badge issuance.

C. TO Contractor shall remove any TO Contractor Personnel from working on the Task Order where the State determines, in its sole discretion, that said TO Contractor Personnel has not adhered to the Security requirements specified herein.

D. The State reserves the right to request that the TO Contractor submit proof of employment authorization of non-United States Citizens, prior to commencement of work under the Task Order.

E. Unless otherwise specified, the cost of complying with all security requirements specified herein are the sole responsibility and obligation of the TO Contractor and its subcontractors and no such costs shall be passed through to or reimbursed by the State or any of its agencies or units.

3.7.2 Security Clearance / Criminal Background Checks

A. The TO Contractor shall obtain from all Contractor Personnel assigned to work on the Task Order a signed statement permitting a criminal background check within thirty (30) days after NTP, the TO Contractor shall secure at its own expense the following type of national criminal history record check and provide the TO Contract Manager with completed checks on such Contractor Personnel prior to assignment.

B. A national criminal history record check. This check may be performed by a public or private entity. The State reserves the right to require, when allowed, a fingerprint-based Maryland and/or FBI Criminal Justice Information System criminal history record check.

C. At a minimum, these background checks must include all convictions and probation before judgment (PBJ) dispositions. The TO Contractor may not assign an individual whose background check reflects any criminal activity to work under this Task Order unless prior written approval is obtained from the TO Contract Manager.

D. TO Contractor shall be responsible for ensuring that TO Contractor Personnel background check certifications are renewed annually, and at the sole expense to the TO Contractor.

E. Further, TO Contractor Personnel may be subject to random security checks during entry and exit of State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while on secured premises.

F. TO Contractor shall complete a criminal background check prior to any individual TO Contractor Personnel being assigned work on the project. TO Contractor shall provide a Criminal Background Check Affidavit (Appendix 3) within 30 days of notice to proceed. On-Site Security Requirement(s)

G. For the conditions noted below, TO Contractor Personnel may be barred from entrance or leaving any site until such time that the State's conditions and queries are satisfied.

   1. TO Contractor Personnel may be subject to random security checks when entering and leaving State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while in secured premises.

   2. Some State sites, especially those premises of the Department of Public Safety and Correctional Services, require each person entering the premises to document and inventory items (such as tools and equipment) being brought onto the site, and to submit to a physical search of his or her person. Therefore, TO Contractor Personnel shall always have available an inventory list of tools being brought onto a site and be prepared to present the inventory list to the State staff or an officer upon arrival for review, as well as present the tools or equipment for inspection. Before leaving the site, the TO Contractor Personnel will again present the inventory list and the tools or equipment for inspection. Upon both entering the site and leaving the site, State staff or a correctional or police officer may search TO Contractor Personnel. Depending upon facility rules, specific tools or personal items may be prohibited from being brought into the facility.

H. Any TO Contractor Personnel who enters the premises of a facility under the jurisdiction of the Agency may be searched, fingerprinted (for the purpose of a criminal history background check), photographed and required to wear an identification card issued by the Agency.

I. Further, TO Contractor Personnel shall not violate Md. Code Ann., Criminal Law Art. Section 9-410 through 9-417 and such other security policies of the agency that controls the facility to which the TO Contractor Personnel seeks access. The failure of any of the TO Contractor Personnel to comply with any provision of the TO Agreement is sufficient grounds for the State to immediately terminate the TO Agreement for default.

3.7.3 Information Technology

The TO Contractor shall:

A. Implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry best practices for information security such as those listed below (see **Section 3.7.4**);

B. Ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of the TO Agreement; and

C. The TO Contractor, and TO Contractor Personnel, shall (i) abide by all applicable federal, State and local laws, rules and regulations concerning security of Information Systems and Information Technology and (ii) comply with and adhere to the State IT Security Policy and Standards as each may be amended or revised from time to time. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy, and (iii) the MDOT Information Security Plan in **Appendix 5**.

3.7.4 Data Protection and Controls

TO Contractor shall ensure a secure environment for all State data and any hardware and software (including but not limited to servers, network and data components) to be provided or used in connection with the performance of the TO Agreement and shall apply or cause application of appropriate controls so as to maintain such a secure environment ("Security Best Practices"). Such Security Best Practices shall comply with an accepted industry standard, such as the NIST cybersecurity framework.

A. To ensure appropriate data protection safeguards are in place, the TO Contractor shall implement and maintain the following controls at all times throughout the term of the TO Agreement (the TO Contractor may augment this list with additional controls):

   1. By default, "deny all" and only allow access by exception.

   2. Ensure TO Contractor's Personnel shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The TO Contractor/subcontractor shall complete any necessary paperwork as directed and coordinated with the TO Agreement Monitor to obtain approval by the State to connect TO Contractor/subcontractor-owned equipment to a State LAN/WAN.

3.7.5 Additional security requirements may be established in a Work Order.

3.7.6 The State shall, at its discretion, have the right to review and assess the Contractor's compliance to the security requirements and standards defined in the TO Agreement.

3.7.7 Provisions in Sections 3.7.1 – 3.7.5 shall survive expiration or termination of the TO Agreement. Additionally, the TO Contractor and shall flow down the provisions of Sections 3.7.4-3.7.6 (or the substance thereof) in all subcontracts.

3.8 RESERVED

3.9 SOC 2 Type 2 Audit Report

A SOC 2 Type 2 Report is not a TO Contractor requirement for this Task Order.

3.10 Performance and Personnel

3.10.1 ROLES AND RESPONSIBILITIES

Personnel roles and responsibilities under the Task Order:

A. **TO Procurement Officer** – The TO Procurement Officer has the primary responsibility for the management of the TORFP process, for the resolution of TO Agreement scope issues, and for authorizing any changes to the TO Agreement.

B. **TO Manager -** The TO Manager has the primary responsibility for the management of the work performed under the TO Agreement, administrative functions, including issuing written directions, and for ensuring compliance with the terms and conditions of the CATS+ Master Contract.

   The TO Manager will assign tasks to the personnel provided under this TORFP and will track and monitor the work being performed through the monthly accounting of hours' deliverable for work types; actual work produced will be reconciled with the hours reported.

C. **TO Contractor** – The TO Contractor is the CATS+ Master Contractor awarded this Task Order. The TO Contractor shall provide human resources as necessary to perform the services described in this TORFP Scope of Work.

D. **TO Contractor Manager** – The TO Contractor Manager will serve as primary point of contact with the TO Manager to regularly discuss progress of tasks, upcoming tasking, historical performance, and resolution of any issues that may arise pertaining to the TO Contractor Personnel. The TO Contractor Manager will serve as liaison between the TO Manager and the senior TO Contractor management.

E. **TO Contractor Personnel** – Any official, employee, agent, Subcontractor, or Subcontractor agents of the TO Contractor who is involved with the Task Order over the course of the Task Order period of performance.

F. **Key Personnel** – A subset of TO Contractor Personnel whose departure during the performance period, will, in the State's opinion, have a substantial negative impact on Task Order performance. Key Personnel proposed as part of the TO Proposal shall start as of TO Agreement issuance unless specified otherwise in this TORFP or the Offeror's TO Technical Proposal. Key Personnel may be identified after Task Order award

G. **MDOT Contract Management Office (CMO) -** The CMO is responsible for contract management issues outside of the day to day management of the TO contract after award.

3.10.2 Offeror Experience

The following Offeror experience is expected and will be evaluated as part of the TO Technical Proposal (see the Offeror experience, capability and references evaluation factor from **Section 6.2**):

A. The extent to which the Offeror demonstrates prior experience providing technical business support services, where more desirable experience includes:

   i. Furnishing services to U.S. based commercial or government entities with at least 1,000 end-users.

   ii. Participating in engagements lasting three (3) or more years

   iii. The extent to which the Customer(s) were satisfied with Offeror's performance

   iv. the number of full-time personnel furnished under the engagement, (where 10 or more is considered ideal experience)

B. The extent to which the Offeror has provided multiple full-time resources possessing a current development platform certification (e.g.: a SalesForce or .Net or PowerBuilder developer certification).

C. Offeror's experience with technical business support projects and services similar to those described in the TORFP, as attested by references furnished in the TO Technical Proposal.

3.10.3 Personnel Experience

The following experience is expected and will be evaluated as part of the TO Technical Proposal and references provided (see the capability of proposed resources evaluation factor from **Section 6.2**):

A. The extent to which the programmers have senior level experience in the respective position.

B. For the Senior .Net programmer role, the extent to which the programmer has C#.Net, ASP.Net and VB.Net experience.

3.10.4 Number of Personnel to Propose

As part of the TO Proposal evaluation, Offerors shall propose exactly four (4) personnel who are expected to be available as of the start date specified in the Notice to Proceed (NTP Date). Offerors shall describe in a Staffing Plan how all of the additional resources shall be acquired to meet the needs of the Agency (see Section 2.3.6).

Offerors may generally describe planned positions in a Staffing Plan. Such planned positions may not be used as evidence of fulfilling personnel minimum qualifications.

3.10.5 Key Personnel Identified

For the Task Order, the following positions will be considered Key Personnel, and shall be required to meet the qualifications stated in Section 1.1 and minimum qualification as referenced in Section 2.10 of the CATS+ Master Contract for selected labor categories.

1. Two (2) Senior .Net Programmers
2. One (1) Senior SalesForce Programmer
3. One (1) Senior Power Builder Programmer

3.10.6 Labor Categories

To be responsive to this TORFP, Offerors must be capable of providing and meeting the minimum qualifications for all the labor categories listed. Offerors shall submit a TO Financial Proposal Form (Attachment B) that provides labor rates for all labor categories for all Task Order years (initial term and any option periods). Actual resumes shall be provided only for Key Personnel as described in **Section 3.10.5**. Resumes for resources provided later shall be coordinated by the TO Manager per the TO Technical Proposal and, if requested in a Work Order, shall be governed by the Work Order process.

A. Each Labor Category includes Titles, Position Description, Education and Experience (General and Specialized).

B. Education and experience described below constitute the minimum qualifications for candidates proposed in response to a TORFP. All experience required must have occurred within the most recent ten (10) years.

C. TO Contractor Personnel Experience (including Key Personnel submitted in response to this TORFP).

3.10.7 Substitution of Education for Experience

A Bachelor's Degree or higher may be substituted for the general and specialized experience for those labor categories requiring a High School Diploma. A Master's Degree may be substituted for two years of the general and specialized experience for those labor categories requiring a Bachelor's Degree. Substitution shall be reviewed and approved by the State at its discretion.

3.10.8 Substitution of Experience for Education

A. Substitution of experience for education may be permitted at the discretion of the State.

B. Substitution of Professional Certificates for Experience:

C. Professional certification (e.g., Microsoft Certified Solutions Expert, SQL Certified Database Administrator) may be substituted for up to two (2) years for general and specialized experience at the discretion of the State.

3.10.9 TO Contractor Personnel Maintain Certifications

Any TO Contractor Personnel provided under this TORFP shall maintain in good standing any required professional certifications for the duration of the TO Agreement.

3.10.10 Work Hours

A. Hours of Operation Support: The TO Contractor shall assign TO Contractor Personnel to support the Agency hours of operation; 08:00 AM to 04:30 PM, Monday through Friday except for MDOT holidays.

B. Needs beyond the hours described in paragraph A may be defined in a Work Order.

C. TO Contractor Personnel may also be required to provide occasional support outside of normal Agency hours of operation, including evenings, overnight, and weekends, to support specific efforts and emergencies, such as to resolve system repair or restoration. Hours performing activities would be billed on an actual time worked basis at the rates proposed.

D. Any work beyond given parameters requires prior approval from the TO Manager is included; an example is: "Unless otherwise directed by the TO Manager, the TO Contractor's assigned personnel will work an eight-hour day (Hours to be approved by TO Manager,) Monday through Friday except for SHA Holidays (including but not limited to Service Reduction Days or Mandatory State Furlough Days)."

E. State-Mandated Closings: TO Contractor Personnel shall be required to participate in any State-mandated closings. In this event, the TO Contractor will be notified in writing by the TO Manager of these details.

F. Minimum and Maximum Hours: Full-time TO Contractor Personnel shall work 40 hours per week with starting and ending times as approved by the TO Manager. A flexible work schedule may be used with TO Manager approval, including time to support any efforts outside core business hours. TO Contractor Personnel may also be requested to restrict the number of hours TO Contractor personnel can work within a given period of time that may result in less than an eight-hour day or less than a 40-hour work week.

G. Vacation Hours: Requests for leave shall be submitted to the TO Manager at least two weeks in advance. The TO Manager reserves the right to request a temporary replacement if leave extends

longer than one consecutive week. In cases where there is insufficient coverage, a leave request may be denied.

3.10.11 Professional Development

Technology and software products continuously change. The TO Contractor shall ensure continuing education opportunities for the personnel provided. This education shall be associated with the technologies currently utilized by SHA or expected to be implemented by SHA in the near future. See also 2.3.4 I

All costs, including, but not limited to, the actual course costs and course attendance time are the responsibility of the TO Contractor. SHA will not reimburse any costs associated with the professional development of TO Contractor Personnel.

The Offeror shall submit a Professional Development Plan as part of the TO Technical Proposal that identifies both annual training course cost allotments as well as annual training time allotments for all resources planned on this Task Order.

3.11 Substitution of Personnel

3.11.1 Directed Personnel Replacement

A. The TO Manager may direct the TO Contractor to replace any TO Contractor Personnel who, in the sole discretion of the TO Manager, are perceived as being unqualified, non-productive, unable to fully perform the job duties, disruptive, or known, or reasonably believed, to have committed a major infraction(s) of law or Agency, Contract, or Task Order requirement.

B. If deemed appropriate in the discretion of the TO Manager, the TO Manager shall give written notice of any TO Contractor Personnel performance issues to the TO Contractor, describing the problem and delineating the remediation requirement(s). The TO Contractor shall provide a written Remediation Plan within three (3) days of the date of the notice. If the TO Manager rejects the Remediation Plan, the TO Contractor shall revise and resubmit the plan to the TO Manager within five (5) days of the rejection, or in the timeframe set forth by the TO Manager in writing. Once a Remediation Plan has been accepted in writing by the TO Manager, the TO Contractor shall immediately implement the Remediation Plan.

C. Should performance issues persist despite the approved Remediation Plan, the TO Manager will give written notice of the continuing performance issues and either request a new Remediation Plan within a specified time limit or direct the removal and replacement of the TO Contractor Personnel whose performance is at issue. A request for a new Remediation Plan will follow the procedure described in **Section 3.11.1.B**.

D. In circumstances of directed removal, the TO Contractor shall provide a suitable replacement for TO Manager approval within fifteen (15) days of the date of the notification of directed removal, or the actual removal, whichever occurs first, or such earlier time as directed by the TO Manager in the event of a removal on less than fifteen days' notice

E. Normally, a directed personnel replacement will occur only after prior notification of problems with requested remediation, as described above. However, the TO Manager reserves the right to direct immediate personnel replacement without utilizing the remediation procedure described above.

F. Replacement or substitution of TO Contractor Personnel under this section shall be in addition to, and not in lieu of, the State's remedies under the Task Order or which otherwise may be available at law or in equity.

G. All Substitutions of personnel require a Criminal Background Check.

3.11.2 Substitution Prior to and 30 Days After Task Order Execution

A. Prior to Task Order Execution or within thirty (30) days after Task Order Execution, the Offeror may substitute proposed Key Personnel only under the following circumstances: vacancy occurs due to the sudden termination, resignation, or approved leave of absence due to an *Extraordinary Personnel Event*, or death of such personnel. To qualify for such substitution, the Offeror must describe to the State's satisfaction the event necessitating substitution and must demonstrate that the originally proposed personnel are actual full-time direct employees with the Offeror (subcontractors, temporary staff or 1099 contractors do not qualify). Proposed substitutions shall be of equal caliber or higher, in the State's sole discretion. Proposed substitutes deemed by the State to be less qualified than the originally proposed individual may be grounds for pre-award disqualification or post-award termination.

B. An *Extraordinary Personnel Event* – means Leave under the Family Medical Leave Act; an incapacitating injury or incapacitating illness; or other circumstances that in the sole discretion of the State warrant an extended leave of absence, such as extended jury duty or extended military service.

3.11.3 Substitution More Than 30 Days After Task Order Execution

The procedure for substituting personnel after Task Order execution is as follows:

A. The TO Contractor may not substitute personnel without the prior approval of the TO Manager.

B. To replace any personnel, the TO Contractor shall submit resumes of the proposed individual specifying the intended approved labor category. Any proposed substitute personnel shall have qualifications equal to or better than those of the replaced personnel.

C. Proposed substitute individual shall be approved by the TO Manager. The TO Manager shall have the option to interview the proposed substitute personnel and may require that such interviews be in person. After the interview, the TO Manager shall notify the TO Contractor of acceptance or denial of the requested substitution. If no acceptable substitute personnel is proposed within the time frame established by the TO Manager, the TO Agreement may be cancelled. A Criminal Background Check is required.

3.12 Minority Business Enterprise (MBE) Reports

3.12.1 MBE PARTICIPATION REPORTS

Agency will monitor both the TO Contractor's efforts to achieve the MBE participation goal and compliance with reporting requirements.

3.12.2 Monthly reporting of MBE participation is required in accordance with the terms and conditions of the CATS+ Master Contract.

D. The TO Contractor shall submit the following reports by the 15th of each month to the Agency at the same time the invoice copy is sent:

2. A Prime Contractor Paid/Unpaid MBE Invoice Report (**Attachment D MDOT MBE Form D-5**) listing any unpaid invoices, over 45 days old, received from any certified MBE subcontractor, the amount of each invoice and the reason payment has not been made; and

3. (If Applicable) An MBE Prime Contractor Report identifying an MBE prime's self-performing work to be counted towards the MBE participation goals.

3.12.3 The TO Contractor shall ensure that each MBE subcontractor provides a completed Subcontractor Paid/Unpaid MBE Invoice Report (**Attachment D MDOT MBE Form D-6**) by the 15th of each month.

3.12.4 Subcontractor reporting shall be sent directly from the subcontractor to the Agency. The TO Contractor shall e-mail all completed forms, copies of invoices and checks paid to the MBE directly to the TO Manager.

3.13 Veteran Small Business Enterprise (VSBE) Reports

There is no VSBE Goal for this Task Order.

3.14 Work Orders

A. Additional services and resources will be provided via a Work Order process. Work shall not begin in advance of a fully executed Work Order. A Work Order may be issued for time and materials (T&M) or fixed pricing. T&M Work Orders will be issued in accordance with pre-approved Labor Categories with the fully loaded rates proposed in **Attachment B**.

B. The TO Manager shall e-mail a Work Order Request (See sample at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+WorkOrderSample.pdf) to the TO Contractor to provide services or resources that are within the scope of this TORFP. The Work Order Request will include:

1. Technical requirements and description of the service or resources needed
2. Performance objectives and/or deliverables, as applicable
3. Due date and time for submitting a response to the request, and
4. Required place(s) where work must be performed

C. The TO Contractor shall e-mail a response to the TO Manager within the specified time and include at a minimum:

1. A response that details the TO Contractor's understanding of the work;
2. A price to complete the Work Order Request using the format provided (see online sample).
3. A description of proposed resources required to perform the requested tasks, with labor categories listed in accordance with Attachment B.
4. An explanation of how tasks shall be completed. This description shall include proposed subcontractors and related tasks.
5. State-furnished information, work site, and/or access to equipment, facilities, or personnel
6. The proposed personnel resources, including any subcontractor personnel, to complete the task.

D. For a T&M Work Order, the TO Manager will review the response and will confirm the proposed labor rates are consistent with this TORFP. For a fixed price Work Order, the TO Manager will review the response and will confirm the proposed prices are acceptable.

E. The TO Manager may contact the TO Contractor to obtain additional information, clarification or revision to the Work Order, and will provide the Work Order to the TO Procurement Officer for a determination of compliance with the TO Agreement and a determination whether a change order is appropriate. Written TO Procurement Officer approval is required before Work Order execution by the State.

F. Proposed personnel on any type of Work Order shall be subject to Agency approval. The TO Contractor shall furnish resumes of proposed personnel specifying the labor category(ies) proposed.

The TO Manager shall have the option to interview the proposed personnel and, in the event of an interview or not, shall notify the TO Contractor of acceptance or denial of the personnel.

G. Performance of services under a Work Order shall commence consistent with an NTP issued by the TO Manager for such Work Order.

3.15 Additional Clauses

The TO Contractor shall be subject to the requirements in this section and shall flow down the provisions of **Sections 3.15.1 – 3.15.8**(or the substance thereof) in all subcontracts.

3.15.1 TORFP Subject to CATS+ Master Contract

In addition to the requirements of this TORFP, the Master Contractors are subject to all terms and conditions contained in the CATS+ RFP issued by the Maryland Department of Information Technology (DoIT) and subsequent Master Contract Project Number 060B2490023, including any amendments, including but not limited to:

A. Custom Software, Custom Source Code, Data;

B. Hardware and software costs procured as part of the TORFP cannot exceed 49 percent of the total Task Order value;

C. Material costs shall be passed through with no mark-up by the TO Contractor;

D. Non-Visual Access

E. By responding to this TORFP and accepting a Task Order award, an Offeror specifically agrees that for any software, hardware or hosting service that it proposes for use by the State in response to this TORFP, the State will have the right to purchase from another source, instead of from the selected Offeror.

3.15.2 All times specified in this document are local time, defined as Eastern Standard Time or Eastern Daylight Time, whichever is in effect.

3.15.3 Contract Management Oversight Activities

A. DoIT is responsible for contract management oversight on the CATS+ Master Contract. As part of that oversight, DoIT has implemented a process for self-reporting contract management activities of Task Orders under CATS+. This process typically applies to active TOs for operations and maintenance services valued at $1 million or greater, but all CATS+ Task Orders are subject to review.

B. A sample of the TO Contractor Self-Reporting Checklist is available on the CATS+ website at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+Self-ReportingChecklistSample.pdf. DoIT may send initial checklists out to applicable/selected TO Contractors approximately three months after the award date for a Task Orders. The TO Contractor shall complete and return the checklist as instructed on the form. Subsequently, at six-month intervals from the due date on the initial checklist, the TO Contractor shall update and resend the checklist to DoIT.

3.15.4 Source Code Escrow

Source code Escrow does not apply to this Task Order.

3.15.5 Purchasing and Recycling Electronic Products

This section does not apply to this solicitation.

3.15.6 Change Control and Advance Notice

This section does not apply to this solicitation.

3.15.7 No-Cost Extensions

In the event there are unspent funds remaining on the TO Agreement, prior to the TO's expiration date the TO Procurement Officer may modify the TO Agreement to extend the TO Agreement beyond its expiration date for the performance of work within the TO's scope of work. Notwithstanding anything to the contrary, no funds may be added to the TO Agreement in connection with any such extension.

3.15.8 CERTIFICATION REGARDING DISCRIMINATORY BOYCOTTS OF ISRAEL

TO Proposals must contain a completed certification (Appendix 7) that the Master Contractor: (1) is not engaging in a boycott of Israel and that (2) it will, for the duration of its contractual obligations, refrain from a boycott of Israel.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

4 TORFP Instructions

4.1 TO Pre-Proposal Conference

4.1.1 A TO pre-proposal conference (Conference) will be held at the date, time, and location indicated on the Key Information Summary Sheet.

4.1.2 Attendance at the Conference is not mandatory, but all interested parties are encouraged to attend in order to facilitate better preparation of their proposals.

4.1.3 Following the Conference, the attendance record and summary of the Conference will be distributed via e-mail to all Master Contractors known to have received a copy of this TORFP.

4.1.4 Attendees should bring a copy of the solicitation and a business card to help facilitate the sign-in process.

4.1.5 In order to assure adequate seating and other accommodations at the Conference, please e-mail the Pre-Proposal Conference Response Form (**Attachment A**) no later than the time and date indicated on the form. In addition, if there is a need for sign language interpretation and/or other special accommodations due to a disability, please notify the TO Procurement Officer at least five (5) business days prior to the Conference date. The Agency will make a reasonable effort to provide such special accommodation.

4.1.6 Seating at the Conference will be limited to two (2) attendees per company.

4.2 Questions

4.2.1 All questions shall identify in the subject line the Solicitation Number and Title (J02B8400024 - SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP), and shall be submitted in writing via e-mail to the TO Procurement Officer no later than the date and time specified the Key Information Summary Sheet.

4.2.2 Answers to all questions that are not clearly specific only to the requestor will be provided to all Master Contractors who are known to have received a copy of the TORFP.

4.2.3 The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Agency unless it issues an amendment in writing.

4.3 TO Proposal Due (Closing) Date and Time

4.3.1 TO Proposals, in the number and form set forth in **Section 5 TO Proposal Format**, must be received by the TO Procurement Officer no later than the TO Proposal due date and time indicated on the Key Information Summary Sheet in order to be considered.

4.3.2 Requests for extension of this date or time shall not be granted.

4.3.3 Offerors submitting TO Proposals should allow sufficient delivery time to ensure timely receipt by the TO Procurement Officer. Except as provided in COMAR 21.05.03.02.F and 21.05.02.10, TO Proposals received after the due date and time listed in the Key Information Summary Sheet will not be considered.

4.3.4 The date and time of an e-mail submission is determined by the date and time of arrival in the e-mail address indicated on the Key Information Summary Sheet.

4.3.5 TO Proposals may be modified or withdrawn by written notice received by the TO Procurement Officer before the time and date set forth in the Key Information Summary Sheet for receipt of TO Proposals.

4.4 Award Basis

Based upon an evaluation of TO Proposal responses as provided in **Section 6.4**, below, a Master Contractor will be selected to conduct the work defined in **Sections 2** and **3**. A specific TO Agreement, **Attachment M**, will then be entered into between the State and the selected Master Contractor, which will bind the selected Master Contractor (TO Contractor) to the contents of its TO Proposal, including the TO Financial Proposal.

4.5 Oral Presentation

4.5.1 Offerors and proposed TO Contractor Personnel will be required to make an oral presentation to State representatives. Offerors must confirm in writing any substantive oral clarification of, or change in, their Proposals made in the course of discussions. Any such written clarifications or changes then become part of the Master Contractor's TO Proposal. The TO Procurement Officer will notify Offerors of the time and place of oral presentations and interviews, should interviews be scheduled separately.

4.5.2 All proposed personnel for Offerors meeting minimum qualifications shall participate in interviews, which are a type of oral presentation. All candidates shall be interviewed in substantially the same manner. The TO Procurement Officer shall, for each round of interviews, determine whether phone or in-person interviews will be utilized. At the TO Procurement Officer's discretion, interviews may be conducted via the internet (e.g., Skype, GotoMeeting, WebEx) in lieu of in-person interviews.

4.6 Limitation of Liability

The TO Contractor's liability is limited in accordance with the Limitations of Liability section of the CATS+ Master Contract. TO Contractor's liability for this TORFP is limited to One (1) times the total TO Agreement amount.

4.7 MBE Participation Goal

4.7.1 A Master Contractor that responds to this TORFP shall complete, sign, and submit all required MBE documentation at the time of TO Proposal submission (See **Attachment D** Minority Business Enterprise Forms). **Failure of the Master Contractor to complete, sign, and submit all required MBE documentation at the time of TO Proposal submission will result in the State's rejection of the Master Contractor's TO Proposal.**

4.7.2 In 2014, Maryland adopted new regulations as part of its Minority Business Enterprise (MBE) program concerning MBE primes. Those new regulations, which became effective June 9, 2014 and are being applied to this task order, provide that when a certified MBE firm participates as a prime contractor on a contract, an agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own forces toward fulfilling up to fifty-percent (50%) of the MBE participation goal (overall) and up to one hundred percent (100%) of not more than one of the MBE participation sub-goals, if any, established for the contract. Please see the attached MBE forms and instructions.

4.8 VSBE Goal

There is no VSBE participation goal for this procurement.

4.9 Living Wage Requirements

The Master Contractor shall abide by the Living Wage requirements under Title 18, State Finance and Procurement Article, Annotated Code of Maryland and the regulations proposed by the Commissioner of Labor and Industry.

All TO Proposals shall be accompanied by a completed Living Wage Affidavit of Agreement, **Attachment F** of this TORFP.

4.10 Federal Funding Acknowledgement

This Task Order does not contain federal funds.

4.11 Conflict of Interest Affidavit and Disclosure

4.11.1 Offerors shall complete and sign the Conflict of Interest Affidavit and Disclosure (**Attachment H**) and submit it with their Proposals. All Offerors are advised that if a TO Agreement is awarded as a result of this solicitation, the TO Contractor's Personnel who perform or control work under this TO Agreement and each of the participating subcontractor personnel who perform or control work under this TO Agreement shall be required to complete agreements substantially similar to **Attachment H**, conflict of interest Affidavit and Disclosure.

4.11.2 If the TO Procurement Officer makes a determination that facts or circumstances exist that give rise to or could in the future give rise to a conflict of interest within the meaning of COMAR 21.05.08.08A, the TO Procurement Officer may reject an Offeror's TO Proposal under COMAR 21.06.02.03B.

4.11.3 Master Contractors should be aware that the State Ethics Law, Md. Code Ann., General Provisions Article, Title 5, might limit the selected Master Contractor's ability to participate in future related procurements, depending upon specific circumstances.

4.11.4 By submitting a Conflict of Interest Affidavit and Disclosure, the Offeror shall be construed as certifying all TO Contractor Personnel and Subcontractors are also without a conflict of interest as defined in COMAR 21.05.08.08A.

4.12 Non-Disclosure Agreement

4.12.1 Non-Disclosure Agreement (Offeror)

A Non-Disclosure Agreement (Offeror) is not required for this solicitation.

4.12.2 Non-Disclosure Agreement (TO Contractor)

All Offerors are advised that this solicitation and any TO Agreement(s) are subject to the terms of the Non-Disclosure Agreement (NDA) contained in this solicitation as **Attachment I**. This Agreement must be provided within five (5) Business Days of notification of recommended award; however, to expedite processing, it is suggested that this document be completed and submitted with the TO Proposal.

4.13 HIPAA - Business Associate Agreement

A HIPAA Business Associate Agreement is not required for this procurement.

4.14 Iranian Non-Investment

All TO Proposals shall be accompanied by a completed Certification Regarding Investments in Iran, **Attachment N** of this TORFP.

4.15 Mercury and Products That Contain Mercury

This solicitation does not include the procurement of products known to likely include mercury as a component.

4.16 Location of the Performance of Services Disclosure

The Offeror is required to complete the Location of the Performance of Services Disclosure. A copy of this Disclosure is included as **Attachment L**. The Disclosure must be provided with the TO Proposal.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

5 TO Proposal Format

5.1 Required Response

Each Master Contractor receiving this CATS+ TORFP shall respond no later than the submission due date and time designated in the Key Information Summary Sheet or as amended. Each Master Contractor is required to submit one of two possible responses: 1) a TO Proposal; or 2) a completed Master Contractor Feedback Form (available online within the Master Contractor Admin System). The feedback form helps the State understand for future contract development why Master Contractors did not submit proposals. The form is accessible via the CATS+ Master Contractor login screen and clicking on TORFP Feedback Response Form from the menu.

A TO Proposal shall conform to the requirements of this CATS+ TORFP.

5.2 Two Part Submission

Offerors shall submit TO Proposals in separate volumes:

- Volume I – TO TECHNICAL PROPOSAL
- Volume II – TO FINANCIAL PROPOSAL

5.3 TO Proposal Packaging and Delivery

5.3.1 TO Proposals delivered by facsimile shall not be considered.

5.3.2 Provide no pricing information in the TO Technical Proposal. Provide no pricing information on the media submitted in the TO Technical Proposal.

5.3.3 Offerors may submit TO Proposals by electronic means as described.

A. Electronic means includes e-mail to the TO Procurement Officer address listed on the Key Information Summary Sheet.

B. An Offeror wishing to deliver a hard copy (paper) TO Proposal shall contact the TO Procurement Officer for instructions.

5.3.4 E-mail submissions

A. All TO Proposal e-mails shall be sent with password protection.

B. The TO Procurement Officer will not accept submissions after the date and exact time stated in the Key Information Summary Sheet. The date and time of submission is determined by the date and time of arrival in the TO Procurement Officer's e-mail box. Time stamps on outgoing email from Master TO Contractors shall not be accepted. Requests for extension of this date or time will not be granted. Except as provided in COMAR 21.05.03.02F, TO Proposals received by the TO Procurement Officer after the due date will not be considered.

C. The State has established the following procedure to restrict access to TO Proposals received electronically: all Technical and TO Financial Proposals must be password protected, and the password for the TO TECHNICAL PROPOSAL must be different from the password for the TO Financial Proposal. Offerors will provide these two passwords to SHA upon request or their TO Proposal will be deemed not susceptible for award. Subsequent submissions of TO Proposal content will not be allowed.

D. The TO Procurement Officer will only contact those Offerors with TO Proposals that are reasonably susceptible for award.

E. TO Proposals submitted via e-mail must not exceed 7 Mb. If a submission exceeds this size, split the submission into two or more parts and include the appropriate part number in the subject (e.g., part 1 of 2) after the subject line information below.

F. The e-mail submission subject line shall state the TORFP J02B8400024 and either "Technical" or "Financial."

5.3.5 Two Part Submission:

A. TO Technical Proposal consisting of:

1. TO Technical Proposal and all supporting material in Microsoft Word format, version 2007 or greater,

2. the TO Technical Proposal in searchable Adobe PDF format,

3. a second searchable Adobe copy of the TO Technical Proposal, redacted in accordance with confidential and/or proprietary information removed (see **Section 5.4.2.B**, and

B. TO Financial Proposal consisting of:

1. TO Financial Proposal and all supporting material in Word format,

2. the TO Financial Proposal in searchable Adobe PDF format,

3. a second searchable Adobe copy of the TO Financial Proposal, redacted in accordance with confidential and/or proprietary information removed (see **Section 5.4.2.B**).

5.4 Volume I - TO Technical Proposal

NOTE: Provide **no pricing information** in the TO Technical Proposal (Volume I). Include pricing information only in the TO Financial Proposal (Volume II).

5.4.1 In addition to the instructions below, responses in the Offeror's TO Technical Proposal shall reference the organization and numbering of Sections in the TORFP (e.g., "Section 2.2.1 Response . . .; "Section 2.2.2 Response . . .,"). All pages of both TO Proposal volumes shall be consecutively numbered from beginning (Page 1) to end (Page "x").

5.4.2 The TO Technical Proposal shall include the following documents and information in the order specified as follows:

A. Proposed Services:

1. Executive Summary: A one-page summary describing the Offeror's understanding of the TORFP scope of work (**Sections 2-3**) and proposed solution.

2. Proposed Solution: A more detailed description of the Offeror's understanding of the TORFP scope of work, proposed methodology and solution. The proposed solution shall be organized to exactly match the requirements outlined in Sections 2-3.

3. Professional Development Plan: Provide a summary on the importance of technical training and how the Offeror promotes it. Detail the annual allotted costs per resource in both course fees and time that will elevate their skill set per Section 2.3.4.I. Also detail any training options provided by the Offeror that are available to the resources.

B. Proposer Information Sheet and Transmittal Letter

The Offeror Information Sheet (see **Appendix 2**) and a Transmittal Letter shall accompany the TO Technical Proposal. The purpose of the Transmittal Letter is to transmit the TO Proposal and acknowledge the receipt of any addenda to this TORFP issued before the TO

Proposal due date and time. Transmittal Letter should be brief, be signed by an individual who is authorized to commit the Offeror to its TO Proposal and the requirements as stated in this TORFP, and contain acknowledgement of all addenda to this TORFP issued before the TO Proposal due date.

C. Minimum Qualifications Documentation (If applicable)

Offeror company minimum qualifications do not apply to this TORFP.

D. Proposed Personnel and TORFP Staffing

Offeror shall propose exactly four (4) Key Personnel in response to this TORFP. Offeror shall:

1. Identify the qualifications and types of staff proposed to be utilized under the Task Order. The Offeror shall describe in detail how the proposed staff's experience and qualifications relate to their specific responsibilities, including any staff of proposed subcontractor(s), as detailed in the Work Plan.
2. Complete and provide for each proposed resource **Appendix 3A** Minimum Qualifications Summary and **Appendix 3B** Personnel Resume Form.
3. Provide evidence proposed personnel possess the required certifications in accordance with **Section 1.1** Offeror Personnel Minimum Qualifications. Also provide any specific proof requirements such as an image of the proposed personnel's unexpired certifications.
4. Provide three (3) references per proposed Key Personnel containing the information listed in **Appendix 3B**.
5. Provide a Staffing Management Plan that demonstrates how the Offeror will provide all planned resources (see Section 2.3.6 Number of Personnel to Propose) in addition to the four (4) Key personnel requested in this TORFP, and how the TO Contractor Personnel shall be managed. Include:
   a) Planned team composition by role (**Important! Identify specific names and provide history only for the proposed resources required for evaluation of this TORFP**).
   b) Process and proposed lead time for locating and bringing on board resources that meet the Task Order needs.
   c) Supporting descriptions for all labor categories proposed in response to this TORFP.
   d) Description of approach for quickly substituting qualified personnel after start of the Task Order.
6. Provide the names and titles of the Offeror's management staff who will supervise the personnel and quality of services rendered under this TO Agreement.

E. Subcontractors

Identify all proposed Subcontractors, including MBEs, and their roles in the performance of the scope of work hereunder.

F. Overall Offeror team organizational chart

Provide an overall team organizational chart with all team resources available to fulfill the Task Order scope of work.

G. Master Contractor and Subcontractor Experience and Capabilities

1. Provide up to three examples of engagements or contracts the Master Contractor or Subcontractor, if applicable, has completed that were similar to the requested scope of work. Include contact information for each client organization complete with the following:

   a) Name of organization.

   b) Point of contact name, title, e-mail and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

   c) Services provided as they relate to the scope of work.

   d) Start and end dates for each example engagement or contract.

   e) Current Master Contractor team personnel who participated on the engagement.

   f) If the Master Contractor is no longer providing the services, explain why not.

2. State of Maryland Experience: If applicable, the Master Contractor shall submit a list of all contracts it currently holds or has held within the past five years with any entity of the State of Maryland.

   For each identified contract, the Master Contractor shall provide the following (if not already provided in sub paragraph A above):

   a) Contract or task order name

   b) Name of organization.

   c) Point of contact name, title, e-mail, and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

   d) Start and end dates for each engagement or contract. If the Master Contractor is no longer providing the services, explain why not.

   e) Dollar value of the contract.

   f) Indicate if the contract was terminated before the original expiration date.

   g) Indicate if any renewal options were not exercised.

Note - State of Maryland experience can be included as part of **G.1** above as engagement or contract experience. State of Maryland experience is neither required nor given more weight in proposal evaluations.

H. State Assistance

Provide an estimate of expectation concerning participation by State personnel.

I. Confidentiality

A Master Contractor should give specific attention to the identification of those portions of its proposal that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Public Information Act, Title 4, of the General Provisions Article of the Annotated Code of Maryland. Master Contractors are advised

that, upon request for this information from a third party, the TO Procurement Officer will be required to make an independent determination regarding whether the information may be disclosed.

Offeror shall furnish a list that identifies each section of the TO Technical Proposal where, in the Offeror's opinion, the Offeror's response should not be disclosed by the State under the Public Information Act.

J. Additional Submissions:

1. Attachments and Exhibits;

a) All forms required for the TO Technical Proposal are identified in **Table 1 of Section 7** – Exhibits and Attachments. Unless directed otherwise by instructions within an individual form, complete, sign, and include all required forms in the TO Technical Proposal.

b) No attachment forms shall be altered. Signatures shall be clearly visible.

5.5 Volume II – TO Financial Proposal

5.5.1 The TO Financial Proposal shall contain all price information in the format specified in **Attachment B -** Financial Proposal Form. The Offeror shall complete the Financial Proposal Form only as provided in the Financial Proposal Form Instructions and the Financial Proposal Form itself.

5.5.2 The TO Financial Proposal shall contain a description of any assumptions on which the Master Contractor's TO Financial Proposal is based (Assumptions shall not constitute conditions, contingencies, or exceptions to the Financial Proposal Form);

5.5.3 **Attachment B**– Financial Proposal Form, with all proposed labor categories including all rates fully loaded. Master Contractors shall list all key resources by approved CATS+ labor categories in the TO Financial Proposal.

5.5.4 To be responsive to this TORFP, the Financial Proposal Form shall provide labor rates for all labor categories anticipated for this TORFP. Proposed rates shall not exceed the rates defined in the Master Contract for the Master Contract year(s) in effect at the time of the TO Proposal due date.

5.5.5 **Note: Failure to specify a CATS+ labor category in the completed Financial Proposal Form for each proposed resource will make the TO Proposal non-responsive to this TORFP.**

5.5.6 Prices shall be valid for 120 days.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

6 Evaluation and Selection Process

The TO Contractor will be selected from among all eligible Master Contractors within the appropriate Functional Area responding to the CATS+ TORFP. In making the TO Agreement award determination, the Agency will consider all information submitted in accordance with Section 5.

6.1 Evaluation Committee

Evaluation of TO Proposals will be performed in accordance with COMAR 21.05.03 by a committee established for that purpose and based on the evaluation criteria set forth below. The Evaluation Committee will review TO Proposals, participate in Offeror oral presentations and discussions, and provide input to the TO Procurement Officer. The Agency reserves the right to utilize the services of individuals outside of the established Evaluation Committee for advice and assistance, as deemed appropriate.

During the evaluation process, the TO Procurement Officer may determine at any time that a particular Offeror is not susceptible for award.

6.2 TO Technical Proposal Evaluation Criteria

The criteria to be used to evaluate each TO Technical Proposal are listed below in descending order of importance. Unless stated otherwise, any sub-criteria within each criterion have equal weight.

6.2.1 Offeror's Technical Response to TORFP Requirements (See TORFP **§ 5.4.2**)

The State prefers an Offeror's response to work requirements in the TORFP that illustrates a comprehensive understanding of work requirements and mastery of the subject matter, including an explanation of how the work will be performed. TO Proposals which include limited responses to work requirements such as "concur" or "will comply" will receive a lower ranking than those TO proposals that demonstrate an understanding of the work requirements and include plans to meet or exceed them.

6.2.2 Experience and Qualifications of Proposed Staff (See TORFP **§ 5.4.2.D**)

The capability of the proposed resources to perform the required tasks and produce the required deliverables in the TORFP **Sections 2-3**. Capability will be determined from each proposed individual's resume, reference checks, and oral presentation (See **Section 4.5** Oral Presentation).

6.2.3 Offeror Qualifications and Capabilities, including proposed subcontractors (See TORFP **§** 5.4.2.G)

a. The State prefers an Offeror's response to its qualifications and capabilities that include specifically programmer experience with the multiple programming languages as specified in Section 2.3.6.

b. References able to attest to the Offeror's experience with staffing contracts for projects and/or services as referenced in the TORFP.

6.2.4 Demonstration of how the Master Contractor plans to staff the task order at the levels set forth in the TORFP and also for potential future resource requests.

6.2.5 Response to the Professional Development Plan as specified in Section 3.10.11, 2.3.4 I.

6.3 TO Financial Proposal Evaluation Criteria

All Qualified Offerors (see **Section 6.4**) will be ranked from the lowest (most advantageous) to the highest (least advantageous) price based on the Total Proposal Price within the stated guidelines set forth in this TORFP and as submitted on **Attachment B** - TO Financial Proposal Form.

6.4 Selection Procedures

TO Technical Proposals shall be evaluated based on the criteria set forth above in **Section 6.2**. TO Technical Proposals and TO Financial Proposals will be evaluated independently of each other.

A. TO Proposals will be assessed throughout the evaluation process for compliance with the minimum qualifications listed in Section 1 of this TORFP, and quality of responses to **Section 5.3** TO Technical Proposal. Failure to meet the minimum qualifications shall render a TO Proposal not reasonably susceptible for award. The TO Procurement Officer will notify those Offerors who have not been selected to perform the work.

B. TO Technical Proposals will be evaluated for technical merit and ranked. At the State's sole discretion, a down-select procedure may be followed as described in 6.4.1 below. Oral presentations and discussions may be held to assure full understanding of the State's requirements and of the qualified Offeror's proposals and abilities to perform, and to facilitate arrival at a TO Agreement that is most advantageous to the State.

C. The Procurement Officer will only open the TO Financial Proposals where the associated TO Technical Proposals have been classified as reasonably susceptible for award.

D. After review of TO Financial Proposals, TO Financial Proposals for qualified Offerors will be reviewed and ranked from lowest to highest price proposed.

E. When in the best interest of the State, the TO Procurement Officer may permit Qualified Offerors to revise their initial Proposals and submit, in writing, Best and Final Offers (BAFOs). The State may make an award without issuing a request for a BAFO.

F. The Procurement Officer shall make a determination recommending award of the TO to the responsible Offeror who has the TO Proposal determined to be the most advantageous to the State, considering price and the evaluation criteria set forth above. In making this selection, the TO Technical Proposal will be given greater weight than the TO Financial Proposal.

All Master Contractors submitting a TO Proposal shall receive written notice from the TO Procurement Officer identifying the awardee.

6.4.1 Down-Select Procedure

In the event that more than ten (10) qualified TO Proposals are received, the TO Procurement Officer may elect to follow a down-select process as follows:

A. A technical ranking will be performed for all TO Proposals based on the resumes submitted. TO Proposals will be ranked from highest to lowest for technical merit based on the quality of the resumes submitted and the extent to which the proposed individuals' qualifications align with the position needs as described in this TORFP.

B. The top ten (10) TO Proposals identified by the technical ranking will be invited to interviews. All other Offerors will be notified of non-selection for this TORFP.

6.5 Documents Required upon Notice of Recommendation for Task Order Award

Upon receipt of a Notification of Recommendation for Task Order award, the apparent awardee shall complete and furnish the documents and attestations as directed in Table 1 of **Section 7 – TORFP Attachments and Appendices**.

Commencement of work in response to a TO Agreement shall be initiated only upon the completed documents and attestations, plus:

A. Issuance of a fully executed TO Agreement,

B. Purchase Order, and

C. by a Notice to Proceed authorized by the TO Manager. See (see online example at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+NoticeToProceedSample.pdf).

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

7 TORFP ATTACHMENTS AND APPENDICES

Instructions Page

A TO Proposal submitted by an Offeror must be accompanied by the completed forms and/or affidavits identified as "with proposal" in the "When to Submit" column in Table 1 below. All forms and affidavits applicable to this TORFP, including any applicable instructions and/or terms, are identified in the "Applies" and "Label" columns in Table 1.

For documents required as part of the proposal:

A. For e-mail submissions, submit one (1) copy of each with signatures.

B. For paper submissions, submit two (2) copies of each with original signatures. All signatures must be clearly visible.

All Offerors are advised that if a Task Order is awarded as a result of this solicitation, the successful Offeror will be required to complete certain forms and affidavits after notification of recommended award. The list of forms and affidavits that must be provided is described in Table 1 below in the "When to Submit" column.

For documents required after award, submit three (3) copies of each document within the appropriate number of days after notification of recommended award, as listed in Table 1 below in the "When to Submit" column.

Table 1: TORFP ATTACHMENTS AND APPENDICES

Applies?	When to Submit	Label	Attachment Name
Y	Before TO Proposal	A	Pre-Proposal Conference Response Form
Y	With TO Proposal	B	TO Financial Proposal Instructions and Form
N	n/a	C	RESERVED
Y	With TO Proposal	D	MDOT MBE Forms A and B **Important:** MDOT MBE Form E, if a waiver has been requested, is also required with TO Proposal
Y	Within 10 days after recommended award	D	MDOT MBE Forms C and D
Y	As directed in forms	D	MDOT MBE Forms D-5 and D-6
N	With TO Proposal	E	Veteran-Owned Small Business Enterprise (VSBE) Form E-1
N	5 Business Days after recommended award	E	VSBE Forms E-1B, E-2, E-3
Y	With TO Proposal	F	Maryland Living Wage Requirements for Service Task Orders and Affidavit of Agreement
N	With TO Proposal	G	Federal Funds Attachments
Y	With TO Proposal	H	Conflict of Interest Affidavit and Disclosure

Applies?	When to Submit	Label	Attachment Name
Y	5 Business Days after recommended award	I	Non-Disclosure Agreement (TO Contractor)
N	5 Business Days after recommended award	J	HIPAA Business Associate Agreement
N	With TO Proposal	K	Mercury Affidavit
Y	With TO Proposal	L	Location of the Performance of Services Disclosure
Y	5 Business Days after recommended award	M	Task Order Agreement
Y	With TO Proposal	N	Certification regarding Investments in Iran
Appendices			
Applies?	**When to Submit**	**Label**	**Attachment Name**
Y	N/A	1	Abbreviations and Definitions
Y	With TO Proposal	2	Offeror Information Sheet
Y	With TO Proposal	3	Labor Classification Personnel Resume Summary (Appendix 3A and 3B)
Y	Within 30 days after NTP Date	4	Criminal Background Check Affidavit
Y	N/A	5	Maryland Department of Transportation Information Security Policy
Y	After NTP Date	6	Weekly TO Contract Personnel Status Report
Y	With TO Proposal	8	Certification Regarding Discriminatory Boycotts of Israel
Additional Submissions			
Applies?	**When to Submit**	**Label**	**Attachment Name**
Y	5 Business Days after recommended award	--	Evidence of meeting insurance requirements (see **Section 3.6**); 1 copy

Attachment A. TO Pre-Proposal Conference Response Form

Solicitation Number J02B8400024

SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP

A TO Pre-proposal conference will be held on Wednesday, 4/11/2018 at 10:00 AM -11:30 AM (EST), at Maryland Department of Transportation, TSO, 4th Floor Board Room.

Please return this form

to Peggy Tischler at ptischler@mdot.state.md.us no later than 2:00 PM on Monday, 4/9/2018 by close of business advising whether or not you plan to attend. The completed form should be returned via e-mail or fax to the Procurement Officer at the contact information below:

Peggy Tischler

MDOT
E-mail: ptischler@mdot.state.md.us;
Fax #: 410-865-1388

Please indicate:

_____ Yes, the following representatives will be in attendance.
Attendees (attendance is limited to 2 attendees from each Firm):
1.

2.

_____ No, we will not be in attendance.

Please specify whether any reasonable accommodations are requested (see TORFP § 4.1"TO Pre-proposal conference"):

Offeror: _____
Offeror Name (please print or type)

By: _____
Signature/Seal

Printed Name: _____
Printed Name

Title: _____
Title

Date: _____
Date

DIRECTIONS TO THE TO PRE-PROPOSAL CONFERENCE

Maryland Department of Transportation
Headquarters
7201 Corporate Center Drive
Hanover MD 21076
410-865-1000
Toll Free 1-888-713-1414

From the South
From I-97 take MD 100 West to MD 170 North. Take MD 170 North to Stoney Run. Take the ramp that veers to the right. Make a left at the top of the ramp and cross over MD 170. Proceed to the next light this will be the New Ridge Road intersection, turn right Corporate Center Drive begins. MDOT Headquarters is ¾ mile on the right side of the road. Visitor parking is to the left.

From the North
From I-95 or BW Parkway take I-195 to MD 170 South to Stoney Run. Turn left at the light. Make a left at the top of the ramp and cross over MD 170. Proceed to the next light this will be the New Ridge Road intersection, turn right Corporate Center Drive begins. MDOT Headquarters is ¾ mile on the right side of the road. Visitor parking is to the left.

Marc Train Service
Ride the Marc Penn Line Train from both the South and North and exit at the BWI Marc Train Station. When you exit the train follow directions to the crossover (tracks) and you will find an exit door on the second floor leading to a pedestrian bridge. This pedestrian bridge will carry you (1600 ft.) to MDOT

Light Rail Service
Ride the light rail from the North to the BWI Airport Station. There is shuttle service from the BWI Airport to BWI Marc Train Station. Take the crossover (tracks) and on the second floor there is an exit to the Pedestrian Bridge for MDOT. This pedestrian bridge will carry you (1600 ft.) to MDOT

Attachment B. TO Financial Proposal Instructions & Form

B-1 FINANCIAL PROPOSAL INSTRUCTIONS

In order to assist Offerors in the preparation of their Financial Proposal and to comply with the requirements of this solicitation, Financial Proposal Instructions and a Financial Proposal Form have been prepared. Offerors shall submit their Financial Proposal on the Financial Proposal Form in accordance with the instructions on the Financial Proposal Form and as specified herein. Do not alter the Financial Proposal Form or the Proposal may be determined to be not reasonably susceptible of being selected for award. The Financial Proposal Form is to be signed and dated, where requested, by an individual who is authorized to bind the Offeror to the prices entered on the Financial Proposal Form.

The Financial Proposal Form is used to calculate the Offeror's TOTAL PROPOSAL PRICE. Follow these instructions carefully when completing your Financial Proposal Form:

A) All Unit and Extended Prices must be clearly entered in dollars and cents, e.g., $24.15. Make your decimal points clear and distinct.

B) All Unit Prices must be the actual price per unit the State will pay for the specific item or service identified in this RFP and may not be contingent on any other factor or condition in any manner.

C) All calculations shall be rounded to the nearest cent, i.e., .344 shall be .34 and .345 shall be .35.

D) Any goods or services required through this TORFP and proposed by the vendor at No Cost to the State must be clearly entered in the Unit Price, if appropriate, and Extended Price with $0.00.

E) Every blank in every Financial Proposal Form shall be filled in. Any changes or corrections made to the Financial Proposal Form by the Offeror prior to submission shall be initialed and dated.

F) Except as instructed on the Financial Proposal Form, nothing shall be entered on or attached to the Financial Proposal Form that alters or proposes conditions or contingencies on the prices. Alterations and/or conditions may render the Proposal not reasonably susceptible of being selected for award.

G) It is imperative that the prices included on the Financial Proposal Form have been entered correctly and calculated accurately by the Offeror and that the respective total prices agree with the entries on the Financial Proposal Form. Any incorrect entries or inaccurate calculations by the Offeror will be treated as provided in COMAR 21.05.03.03, and may cause the Proposal to be rejected.

H) If option years are included, Offerors must submit pricing for each option year. Any option to renew will be exercised at the sole discretion of the State and comply with all terms and conditions in force at the time the option is exercised. If exercised, the option period shall be for a period identified in the TORFP at the prices entered in the Financial Proposal Form.

I) All Financial Proposal prices entered below are to be fully loaded prices that include all costs/expenses and/or fees associated with the provision of services as required by the RFP. The Financial Proposal price shall include, but is not limited to, all: labor, profit/overhead,

general operating, administrative, and all other expenses and costs necessary to perform the work set forth in the solicitation. No other amounts will be paid to the Contractor. If labor rates are requested, those amounts shall be fully-loaded rates; no overtime amounts will be paid.

J) Unless indicated elsewhere in the TORFP, sample amounts used for calculations on the Financial Proposal Form are typically estimates for evaluation purposes only. Unless stated otherwise in the TORFP, the Department does not guarantee a minimum or maximum number of units or usage in the performance of this Contract.

K) Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

B-1 FINANCIAL PROPOSAL FORM

The Financial Proposal Form shall contain all price information in the format specified on these pages. Complete the Financial Proposal Form only as provided in the Financial Proposal Instructions. Do not amend, alter or leave blank any items on the Financial Proposal Form. If option years are included, Offerors must submit pricing for each option year. Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

The total class hours per year (Column F) are not to be construed as "guaranteed" hours; the total number of hours is an estimate only for purposes of price sheet evaluation.

One CATS+ Labor Category shall be chosen for each Job Title

A year for this Task Order shall be calculated as one calendar year from the NTP Date. **Labor Rate Maximums:** The maximum labor rate that may be proposed for any CATS+ Labor Category shall not exceed the maximum for the CATS+ Master Contract year in effect on the TO Proposal due date.

****ALL LABOR CATEGORIES ARE TO BE SELECTED FROM THE CATS+ MASTER CONTRACT SECTION 2.10**

Job Title from TORFP	CATS+ Labor Category (see Section 2.10) ****To Be Proposed by Master Contractor**	Year 1 Hourly Labor Rate (A)	Year 2 Hourly Labor Rate (B)	Year 3 Hourly Labor Rate (C)	Year 4 Hourly Labor Rate (D)	Year 5 Hourly Labor Rate (E)	Total Class Hours Per Year (F)	Extended Price (G)
A. Senior C#.Net Programmer (4 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	7840	**$**
B. C# Net Programmer (8 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	15680	**$**
C. Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	3920	**$**
D. SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	3920	**$**

Job Title from TORFP	CATS+ Labor Category (see Section 2.10) ****To Be Proposed by Master Contractor**	Year 1 Hourly Labor Rate (A)	Year 2 Hourly Labor Rate (B)	Year 3 Hourly Labor Rate (C)	Year 4 Hourly Labor Rate (D)	Year 5 Hourly Labor Rate (E)	Total Class Hours Per Year (F)	Extended Price (G)
E. Senior PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	1960	**$**
F. PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	$	$	$	$	1960	**$**
Additional Potential Programmers (2) available via Work Order (calculated as an average of all hourly labor rates)	N/A	Offers calculate as A-F Hourly labor rate divided by 6	Offers calculate as A-F Hourly labor rate divided by 6	Offers calculate as A-F Hourly labor rate divided by 6	Offers calculate as A-F Hourly labor rate divided by 6	Offers calculate as A-F Hourly labor rate divided by 6	3920	**$**
						Total Evaluated Price		**$**

Authorized Individual Name

Company Name

Title

Company Tax ID #

Signature

Date

The Hourly Labor Rate is the actual rate the State will pay for services and shall be recorded in dollars and cents. The Hourly Labor Rate cannot exceed the Master Contract Rate but may be lower. Rates shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TO Agreement.

Attachment C. RESERVED

Attachment D. Minority Business Enterprise (MBE) Forms

TO CONTRACTOR MINORITY BUSINESS ENTERPRISE REPORTING REQUIREMENTS

CATS+ TORFP #J02B8400024

These instructions are meant to accompany the customized reporting forms sent to you by the TO Manager. If, after reading these instructions, you have additional questions or need further clarification, please contact the TO Manager immediately.

1. As the TO Contractor, you have entered into a TO Agreement with the State of Maryland. As such, your company/firm is responsible for successful completion of all deliverables under the contract, including your commitment to making a good faith effort to meet the MBE participation goal(s) established for TORFP. Part of that effort, as outlined in the TORFP, includes submission of monthly reports to the State regarding the previous month's MBE payment activity. Reporting forms D-5 (TO Contractor Paid/Unpaid MBE Invoice Report) and D-6 (Subcontractor Paid/Unpaid MBE Invoice Report) are attached for your use and convenience.

2. The TO Contractor must complete a separate Form D-5 (TO Contractor Paid/Unpaid MBE Invoice Report) for each MBE subcontractor for each month of the contract and submit one copy to each of the locations indicated at the bottom of the form. The report is due no later than the 15th of the month following the month that is being reported. For example, the report for January's activity is due no later than the 15th of February. With the approval of the TO Manager, the report may be submitted electronically. Note: Reports are required to be submitted each month, regardless of whether there was any MBE payment activity for the reporting month.

3. The TO Contractor is responsible for ensuring that each subcontractor receives a copy (e-copy of and/or hard copy) of Form D-6 (Subcontractor Paid/Unpaid MBE Invoice Report). The TO Contractor should make sure that the subcontractor receives all the information necessary to complete the form properly, i.e., all of the information located in the upper right corner of the form. It may be wise to customize Form D-6 (upper right corner of the form) for the subcontractor the same as the Form D-5 was customized by the TO Manager for the benefit of the TO Contractor. This will help to minimize any confusion for those who receive and review the reports.

4. It is the responsibility of the TO Contractor to make sure that all subcontractors submit reports no later than the 15th of each month, regardless of whether there was any MBE payment activity for the reporting month. Actual payment data is verified and entered into the State's financial management tracking system from the subcontractor's D-6 report only. Therefore, if the subcontractor(s) do not submit their D-6 payment reports, the TO Contractor cannot and will not be given credit for subcontractor payments, regardless of the TO Contractor's proper submission of Form D-5. The TO Manager will contact the TO Contractor if reports are not received each month from either the prime contractor or any of

the identified subcontractors. The TO Contractor must promptly notify the TO Manager if, during the course of the contract, a new MBE subcontractor is utilized. Failure to comply with the MBE contract provisions and reporting requirements may result in sanctions, as provided by COMAR 21.11.03.13.

MDOT MBE FORM A
STATE-FUNDED CONTRACTS
CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT
PAGE 1 OF 2

This affidavit must be included with the bid/proposal. If the bidder/offeror fails to accurately complete and submit this affidavit as required, the bid shall be deemed not responsive or the proposal not susceptible of being selected for award.

In connection with the bid/proposal submitted in response to Solicitation No. , I affirm the following:

1. MBE Participation (PLEASE CHECK ONLY ONE)

☐ I have met the overall certified Minority Business Enterprise (MBE) participation goal of percent (%) and the following sub-goals, if applicable:
percent (%) for African American-owned MBE firms
percent (%) for Hispanic American-owned MBE firms
percent (%) for Asian American-owned MBE firms
percent (%) for Women-owned MBE firms
I agree that these percentages of the total dollar amount of the Contract, for the MBE goal and sub-goals (if any), will be performed by certified MBE firms as set forth in the MBE Participation Schedule - Part 2 of the MDOT MBE Form B (State-Funded Contracts).

OR

☐ I conclude that I am unable to achieve the MBE participation goal and/or sub-goals. I hereby request a waiver, in whole or in part, of the overall goal and/or sub-goals. Within 10 business days of receiving notice that our firm is the apparent awardee or as requested by the Procurement Officer, I will submit a written waiver request and all required documentation in accordance with COMAR 21.11.03.11. For a partial waiver request, I agree that certified MBE firms will be used to accomplish the percentages of the total dollar amount of the Contract, for the MBE goal and sub-goals (if any), as set forth in the MBE Participation Schedule - Part 2 of the MDOT MBE Form B (State-Funded Contracts).

2. Additional MBE Documentation

I understand that if I am notified that I am the apparent awardee or as requested by the Procurement Officer, I must submit the following documentation within 10 business days of receiving such notice:
(a) Outreach Efforts Compliance Statement (MDOT MBE Form C - State-Funded Contracts);
(b) Subcontractor Project Participation Statement (MDOT MBE Form D - State-Funded Contracts);
(c) If waiver requested, MBE Waiver Request Documentation and Forms (MDOT MBE/DBE Form E – Good Faith Efforts Guidance and Documentation) per COMAR 21.11.03.11; and

(d) Any other documentation required by the Procurement Officer to ascertain bidder's responsibility/ offeror's susceptibility of being selected for award in connection with the certified MBE participation goal and sub-goals, if any.

I acknowledge that if I fail to return each completed document (in 2 (a) through (d)) within the required time, the Procurement Officer may determine that I am not responsible and therefore not eligible for contract award or that the proposal is not susceptible of being selected for award.

MDOT MBE FORM A
STATE-FUNDED CONTRACTS
CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT
PAGE 2 OF 2

3. Information Provided to MBE firms

In the solicitation of subcontract quotations or offers, MBE firms were provided not less than the same information and amount of time to respond as were non-MBE firms.

4. Products and Services Provided by MBE firms

I hereby affirm that the MBEs are only providing those products and services for which they are MDOT certified.

I solemnly affirm under the penalties of perjury that the information in this affidavit is true to the best of my knowledge, information and belief.

_____	_____
Company Name	Signature of Representative
_____	_____
Address	Printed Name and Title
_____	_____
City, State and Zip Code	Date

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL. IF THE BIDDER/OFFEROR FAILS TO ACCURATELY COMPLETE AND SUBMIT PART 2 WITH THE BID/PROPOSAL AS REQUIRED, THE BID SHALL BE DEEMED NOT RESPONSIVE OR THE PROPOSAL SHALL BE DEEMED NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD.

PLEASE READ BEFORE COMPLETING THIS FORM

1. Please refer to the Maryland Department of Transportation (MDOT) MBE Directory at www.mdot.state.md.us to determine if a firm is certified for the appropriate North American Industry Classification System ("NAICS") Code **and** the product/services description (specific product that a firm is certified to provide or specific areas of work that a firm is certified to perform). For more general information about NAICS, please visit www.naics.com. Only those specific products and/or services for which a prime or subcontractor is a certified MBE in the MDOT Directory can be used for purposes of achieving the MBE participation goals.

2. In order to be counted for purposes of achieving the MBE participation goals, the MBE firm (whether a prime or subcontractor) must be certified for that specific NAICS Code ("MBE" for State-funded projects designation after NAICS Code). **WARNING:** If the firm's NAICS Code is in **graduated status**, such services/products **will not be counted** for purposes of achieving the MBE participation goals. Graduated status is clearly identified in the MDOT Directory (such graduated codes are designated with the word graduated after the appropriate NAICS Code).

3. Examining the NAICS Code is the **first step** in determining whether an MBE firm is certified and eligible to receive MBE participation credit for the specific products/services to be supplied or performed under the contract. The **second step** is to determine whether a firm's Products/Services Description in the MBE Directory includes the products to be supplied and/or services to be performed that are being used to achieve the MBE participation goals. If you have any questions as to whether a firm is certified to perform the specific services or provide specific products, please contact MDOT's Office of Minority Business Enterprise at 1-800-544-6056 or via email at mbe@mdot.state.md.us.

4. Complete the Part 2 – MBE Participation Schedule for all certified MBE firms (including primes and subcontractors) being used to achieve the MBE participation goal and sub-goals, if any.

5. **MBE Prime Self-Performance.** When a certified MBE firm participates as a prime (independently or as part of a joint venture) on a contract, a procurement agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own forces toward fulfilling up to fifty-percent (50%) of the MBE participation goal (overall) and up to one hundred percent (100%) of not more than one of the MBE participation sub-goals, if any, established for the contract. In order to receive credit for self-performance, an MBE prime must be (a) a certified MBE (see 1-3 above) and (b) listed in the Part 2 – MBE Participation Schedule with its certification number, the certification classification under which it will self-perform, and the percentage of the contract that can be counted as MBE self-performance. For the remaining portion of the overall goal and any sub-goals, the MBE prime must also list, in the Part 2 – MBE Participation Schedule, other certified MBE firms used to meet those goals or, after making good faith efforts to obtain the participation of additional MBE firms, request a waiver. Note: A dually-certified MBE firm can use its own forces toward fulfilling ONLY ONE of the MBE sub-goals for which it can be counted.

6. The Contractor's subcontractors are considered second-tier subcontractors. Third-tier contracting used to meet an MBE goal is to be considered the exception and not the rule. The following two conditions must be met before MDOT, its Modal Administrations and the Maryland Transportation Authority may approve a third-tier contracting agreement: (a) the bidder/offeror must request in writing approval of each third-tier contract arrangement, and (b) the request must contain specifics as to why a third-tier contracting arrangement should be approved. These documents must be submitted with the bid/proposal in Part 2 of this MBE Participation Schedule.

7. For each MBE firm that is being used as a supplier/wholesaler/regular dealer/broker/manufacturer, please follow these instructions for calculating the **amount of the subcontract for purposes of achieving the MBE participation goals**:

A. Is the firm certified as a broker of the products/supplies? If the answer is YES, please continue to Item C. If the answer is NO, please continue to Item B.

B. Is the firm certified as a supplier, wholesaler, regular dealer, or manufacturer of such products/supplies? If the answer is YES, continue to Item D. If the answer is NO, continue to Item C only if the MBE firm is certified to perform trucking/hauling services under NAICS Codes 484110, 484121, 484122, 484210, 484220 and 484230. If the answer is NO and the firm is not certified under these NAICS Codes, then no MBE participation credit will be given for the supply of these products.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

C. For purposes of achieving the MBE participation goal, you may count only the amount of any reasonable fee that the MBE firm will receive for the provision of such products/supplies - not the total subcontract amount or the value (or a percentage thereof) of such products and/or supplies. For Column 3 of the MBE Participation Schedule, please divide the amount of any reasonable fee that the MBE firm will receive for the provision of such products/services by the total Contract value and insert the percentage in Line 3.1.

D. Is the firm certified as a manufacturer (refer to the firm's NAICS Code and specific description of products/services) of the products/supplies to be provided? If the answer is NO, please continue to Item E. If the answer is YES, for purposes of achieving the MBE participation goal, you may count the total amount of the subcontract. For Column 3 of the MBE Participation Schedule, please divide the total amount of the subcontract by the total Contract value and insert the percentage in Line 3.1.

E. Is the firm certified as a supplier, wholesaler and/or regular dealer? If the answer is YES and the MBE firm is furnishing and installing the materials and is certified to perform these services, please divide the total subcontract amount (including full value of supplies) by the total Contract value and insert the percentage in Line 3.1. If the answer is YES and the MBE firm is only being used as a supplier, wholesaler and/or regular dealer or is not certified to install the supplies/materials, for purposes of achieving the MBE participation goal, you may only count sixty percent (60%) of the value of the subcontract for these supplies/products (60% Rule). To apply the 60% Rule, first divide the amount of the subcontract for these supplies/products only (not installation) by the total Contract value. Then, multiply the result by sixty percent (60%) and insert the percentage in Line 3.2.

8. For each MBE firm that **is not** being used as a supplier/wholesaler/regular dealer/broker/manufacturer, to calculate the **amount of the subcontract for purposes of achieving the MBE participation goals**, divide the total amount of the subcontract by the total Contract value and insert the percentage in Line 3.1.

Example: $ 2,500 (Total Subcontract Amount) ÷ $10,000 (Total Contract Value) x 100 = 25%

9. **WARNING:** The percentage of MBE participation, computed using the percentage amounts determined per Column 3 for all of the MBE firms listed in Part 2, MUST at least equal the MBE participation goal **and** sub-goals (if applicable) as set forth in MDOT MBE Form A – State-Funded Contracts for this solicitation. If a bidder/offeror is unable to achieve the MBE participation goal and/or any sub-goals (if applicable), then the bidder/offeror must request a waiver in Form A or the bid will be deemed not responsive, or the proposal not susceptible of being selected for award. You may wish to use the attached Goal/Sub-goal Worksheet to assist you in calculating the percentages and confirming that you have met the applicable MBE participation goal and sub-goals (if any).

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

GOAL/SUBGOAL PARTICIPATION WORKSHEET

1. Complete the Part 2 – MBE Participation Schedule for each MBE being used to meet the MBE goal and any sub-goals.

2. After completion of the Part 2 – MBE Participation Schedule, you may use the Goal/Sub-goal Worksheet to calculate the total MBE participation commitment for the overall goal and any sub-goals.

3. **MBE Overall Goal Participation Boxes:** Calculate the total percentage of MBE participation for each MBE classification by adding the percentages determined per Column 3 of the Part 2 – MBE Participation Schedule. Add the percentages determined in Lines 3.1 and 3.2 for the MBE subcontractor (subs) total. Add the overall participation percentages determined in Line 3.3 for the MBE prime total.

4. **MBE Subgoal Participation Boxes:** Calculate the total percentage of MBE participation for each MBE classification by adding the percentages determined per Column 3 of the Part 2 – MBE Participation Schedule. Add the percentages determined in Lines 3.1 and 3.2 for the MBE subcontractor (subs) total. Add the subgoal participation percentages determined in Line 3.3 for the MBE prime total.

5. The percentage amount for the MBE overall participation in the Total MBE Firm Participation Box F1 should be equal to the sum of the percentage amounts in Boxes A through E of the MBE Overall Goal Participation Column of the Worksheet.

6. The percentage amount for the MBE subgoal participation in the Total MBE Firm Participation Box L should be equal to the sum of the percentage amounts in Boxes A through E of the MBE Subgoal Participation Column of the Worksheet.

GOAL/SUBGOAL WORKSHEET		
MBE Classification	**MBE Overall Goal Participation**	**MBE Subgoal Participation**
(A) Total African American Firm Participation (Add percentages determined for African American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(B) Total Hispanic American Firm Participation (Add percentages determined for Hispanic American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(C) Total Asian American Firm Participation (Add percentages listed for Asian American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(D) Total Women-Owned Firm Participation (Add percentages determined for Women-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(E) Total for all other MBE Firms (Add percentages for firms listed as Other MBE Classification per Column 3 of the MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
Total MBE Firm Participation (Add total percentages determined for all MBE Firms in each column of the Worksheet)	**(F1)**_____%	**(F2)**_____%

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 2 – MBE PARTICIPATION SCHEDULE

PAGE __ OF ___

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL. IF THE BIDDER/OFFEROR FAILS TO ACCURATELY COMPLETE AND SUBMIT PART 2 WITH THE BID/PROPOSAL AS REQUIRED, THE BID SHALL BE DEEMED NOT RESPONSIVE OR THE PROPOSAL SHALL BE DEEMED NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD.

Prime Contractor	Project Description	SOLICITATION NUMBER

LIST INFORMATION FOR EACH CERTIFIED MBE PRIME OR MBE SUBCONTRACTOR YOU AGREE TO USE TO ACHIEVE THE MBE PARTICIPATION GOAL AND SUB-GOALS, IF ANY. NOTE INSTRUCTIONS IN EACH COLUMN.

COLUMN 1	**COLUMN 2**	**COLUMN 3** Unless the bidder/offeror requested a waiver in MDOT MBE Form A – State Funded Contracts for this solicitation, the cumulative MBE participation for all MBE firms listed herein must equal at least the MBE participation goal and sub-goals (if applicable) set forth in Form A.
NAME OF MBE PRIME OR MBE SUBCONTRACTOR AND TIER	**CERTIFICATION NO. AND MBE CLASSIFICATION**	FOR PURPOSES OF ACHIEVING THE MBE PARTICIPATION GOAL AND SUB-GOALS, refer to Sections 5 through 8 in Part 1 - Instructions. State the percentage amount of the products/services in Line 3.1, except for those products or services where the MBE firm is being used as a wholesaler, supplier, or regular dealer. For items of work where the MBE firm is being used as a supplier, wholesaler and/or regular dealer, complete Line 3.2 using the 60% Rule. For items of work where the MBE firm is the prime, complete Line 3.3.
MBE Name: _____ ☐ Check here if MBE firm is a subcontractor and complete in accordance with Sections 6, 7, & 8 of Part 1 - Instructions. If this box is checked, complete 3.1 or 3.2 in Column C, whichever is appropriate. ☐ Check here if MBE firm is the prime contractor, including a participant in a joint venture, and self-performance is being counted pursuant to Section 5 of Part 1 - Instructions. If this box is checked, complete 3.3 in Column C. ☐ Check here if MBE firm is a third-tier contractor (if applicable). Please submit written documents in	**Certification Number:** _____ **(If dually certified, check only one box.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____	3.1. **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE- EXCLUDING PRODUCTS/SERVICES FROM SUPPLIERS, WHOLESALERS OR REGULAR DEALERS). **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.2 **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR FOR ITEMS OF WORK WHERE THE MBE FIRM IS BEING USED AS A SUPPLIER, WHOLESALER AND/OR REGULAR DEALER)** (STATE THE PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE AND THEN APPLY THE 60% RULE PER SECTION 7(E) IN PART 1 - INSTRUCTIONS). _____% Total percentage of Supplies/Products **x _____60% (60% Rule)** **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.3. **TOTAL PERCENTAGE TO BE PAID TO MBE PRIME FOR WORK THAT CAN BE COUNTED AS MBE SELF-PERFORMANCE** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE).

accordance with Section 6 of Part 1 - Instructions		**(a)_____% Total percentage for self-performed items of work in which MBE is certified)** **(b)_____% (Insert 50% of MBE overall goal)** **(c)_____% (Insert subgoal for classification checked in Column 2, if applicable)** **Percentages for purposes of calculating achievement of MBE Participation goals:** **➡ For MBE Overall goal – Use lesser of (a) or (b)** **➡ For MBE Subgoal – Use lesser of (a) or (c)** **➡ If MBE Prime is supplier, wholesaler and/or regular dealer, apply the 60% rule.**

☐Check here if Continuation Sheets are attached.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 2 – MBE PARTICIPATION SCHEDULE
CONTINUATION SHEET

PAGE __ OF ___

Prime Contractor	Project Description	1. SOLICITATION NUMBER

LIST INFORMATION FOR EACH CERTIFIED MBE PRIME OR MBE SUBCONTRACTOR YOU AGREE TO USE TO ACHIEVE THE MBE PARTICIPATION GOAL AND SUB-GOALS, IF ANY. NOTE INSTRUCTIONS IN EACH COLUMN.

COLUMN 1	COLUMN 2	COLUMN 3 Unless the bidder/offeror requested a waiver in MDOT MBE Form A – State Funded Contracts for this solicitation, the cumulative MBE participation for all MBE firms listed herein must equal at least the MBE participation goal and sub-goals (if applicable) set forth in Form A.
NAME OF MBE PRIME OR MBE SUBCONTRACTOR AND TIER	**CERTIFICATION NO. AND MBE CLASSIFICATION**	FOR PURPOSES OF ACHIEVING THE MBE PARTICIPATION GOAL AND SUB-GOALS, refer to Sections 5 through 8 in Part 1 - Instructions. State the percentage amount of the products/services in Line 3.1, except for those products or services where the MBE firm is being used as a wholesaler, supplier, or regular dealer. For items of work where the MBE firm is being used as a supplier, wholesaler and/or regular dealer, complete Line 3.2 using the 60% Rule. For items of work where the MBE firm is the prime, complete Line 3.3.
MBE Name: _____ ☐ Check here if MBE firm is a subcontractor and complete in accordance with Sections 6, 7, & 8 of Part 1 - Instructions. If this box is checked, complete 3.1 or 3.2 in Column C, whichever is appropriate. ☐ Check here if MBE firm is the prime contractor, including a participant in a joint venture, and self-performance is being counted pursuant to Section 5 of Part 1 - Instructions. If this box is checked, complete 3.3 in Column C. ☐ Check here if MBE firm is a third-tier contractor (if applicable). Please submit written documents in	**Certification Number:** _____ **(If dually certified, check only one box.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____	3.1. **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE- EXCLUDING PRODUCTS/SERVICES FROM SUPPLIERS, WHOLESALERS OR REGULAR DEALERS). **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.2 **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR FOR ITEMS OF WORK WHERE THE MBE FIRM IS BEING USED AS A SUPPLIER, WHOLESALER AND/OR REGULAR DEALER)** (STATE THE PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE AND THEN APPLY THE 60% RULE PER SECTION 7(E) IN PART 1 - INSTRUCTIONS). _____% Total percentage of Supplies/Products **x _____60% (60% Rule)** **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.3. **TOTAL PERCENTAGE TO BE PAID TO MBE PRIME FOR WORK THAT CAN BE COUNTED AS MBE SELF-PERFORMANCE** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE)..

accordance with Section 6 of Part 1 - Instructions		**(a)_____% Total percentage for self-performed items of work in which MBE is certified)** **(b)_____% (Insert 50% of MBE overall goal)** **(c)_____% (Insert subgoal for classification checked in Column 2, if applicable)** **Percentages for purposes of calculating achievement of MBE Participation goals:** **➡ For MBE Overall goal – Use lesser of (a) or (b)** **➡ For MBE Subgoal – Use lesser of (a) or (c)** **➡If MBE Prime is supplier, wholesaler and/or regular dealer, apply the 60% rule.**

☐Check here if Continuation Sheets are attached.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 3 – CERTIFICATION FOR MBE PARTICIPATION SCHEDULE

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL AS DIRECTED IN THE INVITATION TO BID/ REQUEST FOR PROPOSALS.

I hereby affirm that I have reviewed the Products and Services Description (specific product that a firm is certified to provide or areas of work that a firm is certified to perform) set forth in the MDOT MBE Directory for each of the MBE firms listed in Part 2 of this MBE Form B for purposes of achieving the MBE participation goals and sub-goals that were identified in the MBE Form A that I submitted with this solicitation, and that the MBE firms listed are only performing those products/services/areas of work for which they are certified. I also hereby affirm that I have read and understand the form instructions set forth in Part 1 of this MBE Form B.

The undersigned Prime Contractor hereby certifies and agrees that they have fully complied with the State Minority Business Enterprise law, State Finance and Procurement Article §14-308(a)(2), Annotated Code of Maryland which provides that, except as otherwise provided by law, a contractor may not identify a certified minority business enterprise in a bid or proposal and:

(1) fail to request, receive, or otherwise obtain authorization from the certified minority business enterprise to identify the certified minority business enterprise in its bid or proposal;

(2) fail to notify the certified minority business enterprise before execution of the contract of its inclusion of the bid or proposal;

(3) fail to use the certified minority business enterprise in the performance of the contract; or

(4) pay the certified minority business enterprise solely for the use of its name in the bid or proposal.

I solemnly affirm under the penalties of perjury that the contents of Parts 2 and 3 of MDOT MBE Form B are true to the best of my knowledge, information and belief.

Company Name	Signature of Representative
Address	Printed Name and Title
City, State and Zip Code	Date

MDOT MBE FORM C
STATE-FUNDED CONTRACTS
OUTREACH EFFORTS COMPLIANCE STATEMENT

In conjunction with the offer/proposal submitted in response to Solicitation No._____, I state the following:

1. Bidder/Offeror took the following efforts to identify subcontracting opportunities in these specific work categories:

2. Attached to this form are copies of written solicitations (with bidding/proposal instructions) used to solicit certified MBE firms for these subcontract opportunities.

3. Bidder/Offeror made the following attempts to personally contact the solicited MBE firms:

4. **Please Check One:**

☐ This project does not involve bonding requirements.

☐ Bidder/Offeror assisted MBE firms to fulfill or seek waiver of bonding requirements. (DESCRIBE EFFORTS)

5. **Please Check One:**

☐ Bidder/Offeror did attend the pre-bid/pre-proposal meeting/conference.

☐ No pre-bid/pre-proposal meeting/conference was held.

☐ Bidder/Offeror did not attend the pre-bid/pre-proposal meeting/conference.

_____	_____
Company Name	Signature of Representative
_____	_____
Address	Printed Name and Title
_____	_____
City, State and Zip Code	Date

MDOT MBE FORM D
STATE-FUNDED CONTRACTS
MBE SUBCONTRACTOR PROJECT PARTICIPATION AFFIDAVIT

IF THE BIDDER/OFFEROR FAILS TO RETURN THIS AFFIDAVIT WITHIN THE REQUIRED TIME, THE PROCUREMENT OFFICER MAY DETERMINE THAT THE BIDDER/OFFEROR IS NOT RESPONSIBLE AND THEREFORE NOT ELIGIBLE FOR CONTRACT AWARD OR THAT THE PROPOSAL IS NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD. SUBMIT ONE FORM FOR EACH CERTIFIED MBE FIRM LISTED IN THE MBE PARTICIPATION SCHEDULE. BIDDERS/OFFERORS ARE HIGHLY ENCOURAGED TO SUBMIT FORM D PRIOR TO THE TEN (10) DAY DEADLINE.

Provided that _____ (Prime Contractor's Name) is awarded the State contract in conjunction with Solicitation No. _____, such Prime Contractor will enter into a subcontract with _____(Subcontractor's Name) committing to participation by the MBE firm _____ (MBE Name) with MDOT Certification Number _____ (if subcontractor previously listed is also the MBE firm, please restate name and provide MBE Certification Number) which will receive at least $_____ or ___% (Total Subcontract Amount/ Percentage) for performing the following products/services for the Contract:

NAICS CODE	WORK ITEM, SPECIFICATION NUMBER, LINE ITEMS OR WORK CATEGORIES (IF APPLICABLE)	DESCRIPTION OF SPECIFIC PRODUCTS AND/OR SERVICES

I solemnly affirm under the penalties of perjury that the information provided in this MBE Subcontractor Project Participation Affidavit is true to the best of my knowledge, information and belief. I acknowledge that, for purposes of determining the accuracy of the information provided herein, the Procurement Officer may request additional information, including, without limitation, copies of the subcontract agreements and quotes.

PRIME CONTRACTOR	SUBCONTRACTOR (SECOND-TIER)	SUBCONTRACTOR (THIRD-TIER)
Signature of Representative: _____ __ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____ _____	Signature of Representative: _____ ___ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____	Signature of Representative: _____ ___ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____

Telephone: _____ Date: _____	_____ Telephone: _____ Date: _____	_____ Telephone: _____ Date: _____

IF MBE FIRM IS A THIRD-TIER SUBCONTRACTOR, THIS FORM MUST ALSO BE EXECUTED BY THE SECOND-TIER SUBCONTRACTOR THAT HAS THE SUBCONTRACT AGREEMENT WITH THE MBE FIRM.

This form is to be completed monthly by the prime contractor.

Attachment D-5

Maryland Department of Information Technology
Minority Business Enterprise Participation
Prime Contractor Paid/Unpaid MBE Invoice Report

Report #: _____ Reporting Period (Month/Year): _____ **Report is due to the MBE Officer by the 10th of the month following the month the services were provided.** **Note: Please number reports in sequence**	Contract #: _____ Contracting Unit: _____ Contract Amount: _____ MBE Subcontract Amt: _____ Project Begin Date: _____ Project End Date: _____ Services Provided: _____

Prime Contractor:	Contact Person:	
Address:		
City:	State:	ZIP:
Phone:	FAX:	Email:
Subcontractor Name:	Contact Person:	
Phone:	FAX:	
Subcontractor Services Provided:		

List all payments made to MBE subcontractor named above during this reporting period: **Invoice# Amount** **1.** **2.** **3.** **4.** **Total Dollars Paid: $_____**	**List dates and amounts of any outstanding invoices:** **Invoice # Amount** **1.** **2.** **3.** **4.** **Total Dollars Unpaid: $_____**

**If more than one MBE subcontractor is used for this contract, you must use separate D-5 forms.

****Return one copy (hard or electronic) of this form to the following addresses (electronic copy with signature and date is preferred):**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)

This form must be completed by MBE subcontractor

ATTACHMENT D-6
Minority Business Enterprise Participation
Subcontractor Paid/Unpaid MBE Invoice Report

Report#: ____ Reporting Period (Month/Year): _____ **Report is due by the 10th of the month following the month the services were performed.**	Contract # Contracting Unit: MBE Subcontract Amount: Project Begin Date: Project End Date: Services Provided:

MBE Subcontractor Name:		
MDOT Certification #:		
Contact Person:	Email:	
Address:		
City: Baltimore	State:	ZIP:
Phone:	FAX:	

Subcontractor Services Provided:

List all payments received from Prime Contractor during reporting period indicated above.	**List dates and amounts of any unpaid invoices over 30 days old.**
Invoice Amt **Date**	**Invoice Amt** **Date**
1.	**1.**
2.	**2.**
3.	**3.**
Total Dollars Paid: $_____	**Total Dollars Unpaid: $_____**

Prime Contractor: Contact Person:

****Return one copy of this form to the following address (electronic copy with signature & date is preferred):**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)

Signature: _____ Date: _____
(Required)

ATTACHMENT 2 - MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 1 – Guidance for Demonstrating Good Faith Efforts to Meet MBE/DBE Participation Goals

In order to show that it has made good faith efforts to meet the Minority Business Enterprise (MBE)/Disadvantaged Business Enterprise (DBE) participation goal (including any MBE sub-goals) on a contract, the bidder/offeror must either (1) meet the MBE/DBE Goal(s) and document its commitments for participation of MBE/DBE Firms, or (2) when it does not meet the MBE/DBE Goal(s), document its Good Faith Efforts to meet the goal(s).

I. Definitions

MBE/DBE Goal(s) – "MBE/DBE Goal(s)" refers to the MBE participation goal and MBE participation sub-goal(s) on a State-funded procurement and the DBE participation goal on a federally-funded procurement.

Good Faith Efforts – The "Good Faith Efforts" requirement means that when requesting a waiver, the bidder/offeror must demonstrate that it took all necessary and reasonable steps to achieve the MBE/DBE Goal(s), which, by their scope, intensity, and appropriateness to the objective, could reasonably be expected to obtain sufficient MBE/DBE participation, even if those steps were not fully successful. Whether a bidder/offeror that requests a waiver made adequate good faith efforts will be determined by considering the quality, quantity, and intensity of the different kinds of efforts that the bidder/offeror has made. The efforts employed by the bidder/offeror should be those that one could reasonably expect a bidder/offeror to take if the bidder/offeror were actively and aggressively trying to obtain DBE participation sufficient to meet the DBE contract goal. Mere *pro forma* efforts are not good faith efforts to meet the DBE contract requirements. The determination concerning the sufficiency of the bidder's/offeror's good faith efforts is a judgment call; meeting quantitative formulas is not required.

Identified Firms – "Identified Firms" means a list of the DBEs identified by the procuring agency during the goal setting process and listed in the federally-funded procurement as available to perform the Identified Items of Work. It also may include additional DBEs identified by the bidder/offeror as available to perform the Identified Items of Work, such as DBEs certified or granted an expansion of services after the procurement was issued. If the procurement does not include a list of Identified Firms or is a State-funded procurement, this term refers to all of the MBE Firms (if State-funded) or DBE Firms (if federally-funded) the bidder/offeror identified as available to perform the Identified Items of Work and should include all appropriately certified firms that are reasonably identifiable.

Identified Items of Work – "Identified Items of Work" means the bid items identified by the procuring agency during the goal setting process and listed in the procurement as possible items of work for performance by MBE/DBE Firms. It also may include additional portions of items of work the bidder/offeror identified for performance by MBE/DBE Firms to increase the likelihood that the MBE/DBE Goal(s) will be achieved. If the procurement does not include a list of Identified Items of Work, this term refers to all of the items of work the bidder/offeror identified as possible items of work for performance by MBE/DBE Firms and should include all reasonably identifiable work opportunities.

MBE/DBE Firms – For State-funded contracts, "MBE/DBE Firms" refers to certified **MBE** Firms. Certified MBE Firms can participate in the State's MBE Program. For federally-funded contracts, "MBE/DBE Firms" refers to certified **DBE** Firms. Certified DBE Firms can participate in the federal DBE Program.

II. Types of Actions MDOT will Consider

The bidder/offeror is responsible for making relevant portions of the work available to MBE/DBE subcontractors and suppliers and to select those portions of the work or material needs consistent with the available MBE/DBE subcontractors and suppliers, so as to facilitate MBE/DBE participation. The following is a list of types of actions MDOT will consider as part of the bidder's/offeror's Good Faith Efforts when the bidder/offeror fails to meet the

MBE/DBE Goal(s). This list is not intended to be a mandatory checklist, nor is it intended to be exclusive or exhaustive. Other factors or types of efforts may be relevant in appropriate cases.

A. Identify Bid Items as Work for MBE/DBE Firms

1. Identified Items of Work in Procurements

(a) Certain procurements will include a list of bid items identified during the goal setting process as possible work for performance by MBE/DBE Firms. If the procurement provides a list of Identified Items of Work, the bidder/offeror shall make all reasonable efforts to solicit quotes from MBE Firms or DBE Firms, whichever is appropriate, to perform that work.

(b) Bidders/Offerors may, and are encouraged to, select additional items of work to be performed by MBE/DBE Firms to increase the likelihood that the MBEDBE Goal(s) will be achieved.

2. Identified Items of Work by Bidders/Offerors

(a) When the procurement does not include a list of Identified Items of Work, bidders/offerors should reasonably identify sufficient items of work to be performed by MBE/DBE Firms.

(b) Where appropriate, bidders/offerors should break out contract work items into economically feasible units to facilitate MBE/DBE participation, rather than perform these work items with their own forces. The ability or desire of a prime contractor to perform the work of a contract with its own organization does not relieve the bidder/offeror of the responsibility to make Good Faith Efforts.

B. Identify MBE Firms or DBE Firms to Solicit

1. DBE Firms Identified in Procurements

(a) Certain procurements will include a list of the DBE Firms identified during the goal setting process as available to perform the items of work. If the procurement provides a list of Identified DBE Firms, the bidder/offeror shall make all reasonable efforts to solicit those DBE firms.

(b) Bidders/offerors may, and are encouraged to, search the MBE/DBE Directory to identify additional DBEs who may be available to perform the items of work, such as DBEs certified or granted an expansion of services after the solicitation was issued.

2. MBE/DBE Firms Identified by Bidders/Offerors

(a) When the procurement does not include a list of Identified MBE/DBE Firms, bidders/offerors should reasonably identify the MBE Firms or DBE Firms, whichever is appropriate, that are available to perform the Identified Items of Work.

(b) Any MBE/DBE Firms identified as available by the bidder/offeror should be certified in the appropriate program (MBE for State-funded procurements or DBE for federally-funded procurements)

(c) Any MBE/DBE Firms identified as available by the bidder/offeror should be certified to perform the Identified Items of Work.

C. Solicit MBE/DBEs

1. Solicit <u>all</u> Identified Firms for all Identified Items of Work by providing written notice. The bidder/offeror should:

(a) provide the written solicitation at least 10 days prior to bid opening to allow sufficient time for the MBE/DBE Firms to respond;

(b) send the written solicitation by first-class mail, facsimile, or email using contact information in the MBE/DBE Directory, unless the bidder/offeror has a valid basis for using different contact information; and

(c) provide adequate information about the plans, specifications, anticipated time schedule for portions of the work to be performed by the MBE/DBE, and other requirements of the contract to assist MBE/DBE Firms in responding. (This information may be provided by including hard copies in the written solicitation or by electronic means as described in C.3 below.)

2. "All" Identified Firms includes the DBEs listed in the procurement and any MBE/DBE Firms you identify as potentially available to perform the Identified Items of Work, but it does not include MBE/DBE Firms who are no longer certified to perform the work as of the date the bidder/offeror provides written solicitations.

3. "Electronic Means" includes, for example, information provided *via* a website or file transfer protocol (FTP) site containing the plans, specifications, and other requirements of the contract. If an interested MBE/DBE cannot access the information provided by electronic means, the bidder/offeror must make the information available in a manner that is accessible by the interested MBE/DBE.

4. Follow up on initial written solicitations by contacting DBEs to determine if they are interested. The follow up contact may be made:

(a) by telephone using the contact information in the MBE/DBE Directory, unless the bidder/offeror has a valid basis for using different contact information; or

(b) in writing *via* a method that differs from the method used for the initial written solicitation.

5. In addition to the written solicitation set forth in C.1 and the follow up required in C.4, use all other reasonable and available means to solicit the interest of MBE/DBE Firms certified to perform the work of the contract. Examples of other means include:

(a) attending any pre-bid meetings at which MBE/DBE Firms could be informed of contracting and subcontracting opportunities;

(b) if recommended by the procurement, advertising with or effectively using the services of at least two minority focused entities or media, including trade associations, minority/women community organizations, minority/women contractors' groups, and local, state, and federal minority/women business assistance offices listed on the MDOT Office of Minority Business Enterprise website; and

(c) effectively using the services of other organizations, as allowed on a case-by-case basis and authorized in the procurement, to provide assistance in the recruitment and placement of MBE/DBE Firms.

D. Negotiate With Interested MBE/DBE Firms

Bidders/Offerors must negotiate in good faith with interested MBE/DBE Firms.

1. Evidence of negotiation includes, without limitation, the following:

(a) the names, addresses, and telephone numbers of MBE/DBE Firms that were considered;

(b) a description of the information provided regarding the plans and specifications for the work selected for subcontracting and the means used to provide that information; and

(c) evidence as to why additional agreements could not be reached for MBE/DBE Firms to perform the work.

2. A bidder/offeror using good business judgment would consider a number of factors in negotiating with subcontractors, including DBE subcontractors, and would take a firm's price and capabilities as well as contract goals into consideration.

3. The fact that there may be some additional costs involved in finding and using MBE/DBE Firms is not in itself sufficient reason for a bidder's/offeror's failure to meet the contract DBE goal, as long as such costs are reasonable. Factors to take into consideration when determining whether a MBE/DBE Firm's quote is excessive or unreasonable include, without limitation, the following:

(a) the dollar difference between the MBE/DBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(b) the percentage difference between the MBE/DBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(c) the percentage that the DBE subcontractor's quote represents of the overall contract amount;

(d) the number of MBE/DBE firms that the bidder/offeror solicited for that portion of the work;

(e) whether the work described in the MBE/DBE and Non-MBE/DBE subcontractor quotes (or portions thereof) submitted for review is the same or comparable; and

(f) the number of quotes received by the bidder/offeror for that portion of the work.

4. The above factors are not intended to be mandatory, exclusive, or exhaustive, and other evidence of an excessive or unreasonable price may be relevant.

5. The bidder/offeror may not use its price for self-performing work as a basis for rejecting a MBE/DBE Firm's quote as excessive or unreasonable.

6. The "average of the other subcontractors' quotes received by the" bidder/offeror refers to the average of the quotes received from all subcontractors, except that there should be quotes from at least three subcontractors, and there must be at least one quote from a MBE/DBE and one quote from a Non-MBE/DBE.

7. A bidder/offeror shall not reject a MBE/DBE Firm as unqualified without sound reasons based on a thorough investigation of the firm's capabilities. For each certified MBE/DBE that is rejected as unqualified or that placed a subcontract quotation or offer that the bidder/offeror concludes is not acceptable, the bidder/offeror must provide a written detailed statement listing the reasons for this conclusion. The bidder/offeror also must document the steps taken to verify the capabilities of the MBE/DBE and Non-MBE/DBE Firms quoting similar work.

(a) The factors to take into consideration when assessing the capabilities of a MBE/DBE Firm, include, but are not limited to the following: financial capability, physical capacity to perform, available personnel and equipment, existing workload, experience performing the type of work, conduct and performance in previous contracts, and ability to meet reasonable contract requirements.

(b) The MBE/DBE Firm's standing within its industry, membership in specific groups, organizations, or associations and political or social affiliations (for example union vs. non-union employee status) are not legitimate causes for the rejection or non-solicitation of bids in the efforts to meet the project goal.

E. Assisting Interested MBE/DBE Firms

When appropriate under the circumstances, the decision-maker will consider whether the bidder/offeror:

1. made reasonable efforts to assist interested MBE/DBE Firms in obtaining the bonding, lines of credit, or insurance required by MDOT or the bidder/offeror; and

2. made reasonable efforts to assist interested MBE/DBE Firms in obtaining necessary equipment, supplies, materials, or related assistance or services.

III. Other Considerations

In making a determination of Good Faith Efforts the decision-maker may consider engineering estimates, catalogue prices, general market availability and availability of certified MBE/DBE Firms in the area in which the work is to be performed, other bids or offers and subcontract bids or offers substantiating significant variances between certified MBE/DBE and Non-MBE/DBE costs of participation, and their impact on the overall cost of the contract to the State and any other relevant factors.

The decision-maker may take into account whether a bidder/offeror decided to self-perform subcontract work with its own forces, especially where the self-performed work is Identified Items of Work in the procurement. The decision-maker also may take into account the performance of other bidders/offerors in meeting the contract. For example, when the apparent successful bidder/offeror fails to meet the contract goal, but others meet it, this reasonably raises the question of whether, with additional reasonable efforts, the apparent successful bidder/offeror could have met the goal. If the apparent successful bidder/offeror fails to meet the goal, but meets or exceeds the average MBE/DBE participation obtained by other bidders/offerors, this, when viewed in conjunction with other factors, could be evidence of the apparent successful bidder/offeror having made Good Faith Efforts.

IV. Documenting Good Faith Efforts

At a minimum, a bidder/offeror seeking a waiver of the MBE/DBE Goal(s) or a portion thereof must provide written documentation of its Good Faith Efforts, in accordance with COMAR 21.11.03.11, within 10 business days after receiving notice that it is the apparent awardee. The written documentation shall include the following:

A. Items of Work (Complete Good Faith Efforts Documentation Form E, Part 2)

A detailed statement of the efforts made to select portions of the work proposed to be performed by certified MBE/DBE Firms in order to increase the likelihood of achieving the stated MBE/DBE Goal(s).

B. Outreach/Solicitation/Negotiation

1. The record of the bidder's/offeror's compliance with the outreach efforts prescribed by COMAR 21.11.03.09C (2)(a) through (e) and 49 C.F.R. Part 26, Appendix A. **(Complete Outreach Efforts Compliance Statement)**

2. A detailed statement of the efforts made to contact and negotiate with MBE/DBE Firms including:

(a) the names, addresses, and telephone numbers of the MBE/DBE Firms who were contacted, with the dates and manner of contacts (letter, fax, email, telephone, etc.) **(Complete Good Faith Efforts Form E, Part 3, and submit letters, fax cover sheets, emails, etc. documenting solicitations)**; and

(b) a description of the information provided to MBE/DBE Firms regarding the plans, specifications, and anticipated time schedule for portions of the work to be performed and the means used to provide that information.

C. Rejected MBE/DBE Firms (Complete Good Faith Efforts Form E, Part 4)

1. For each MBE/DBE Firm that the bidder/offeror concludes is not acceptable or qualified, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the steps taken to verify the capabilities of the MBE/DBE and Non-MBE/DBE Firms quoting similar work.

2. For each certified MBE/DBE Firm that the bidder/offeror concludes has provided an excessive or unreasonable price, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the quotes received from all MBE/DBE and Non-MBE/DBE firms bidding on the same or comparable work. **(Include copies of all quotes received.)**

3. A list of MBE/DBE Firms contacted but found to be unavailable. This list should be accompanied by a Minority Contractor Unavailability Certificate signed by the MBE/DBE contractor or a statement from the bidder/offeror that the MBE/DBE contractor refused to sign the Minority Contractor Unavailability Certificate.

D. Other Documentation

1. Submit any other documentation requested by the Procurement Officer to ascertain the bidder's/offeror's Good Faith Efforts.

2. Submit any other documentation the bidder/offeror believes will help the Procurement Officer ascertain its Good Faith Efforts.

ATTACHMENT 2 - MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 2 – Certification Regarding Goof Faith Efforts and Documentation

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

PARTS 3, 4, AND 5 MUST BE INCLUDED WITH THIS CERTIFICATE ALONG WITH ALL DOCUMENTS SUPPORTING YOUR WAIVER REQUEST.

I hereby request a waiver of (1) the Minority Business Enterprise (MBE) participation goal and/or subgoal(s), (2) the Disadvantaged Business Enterprise (DBE) participation goal, or (3) a portion of the pertinent MBE/DBE participation goal and/or MBE subgoal(s) for this procurement.[1] I affirm that I have reviewed the Good Faith Efforts Guidance MBE/DBE Form E. I further affirm under penalties of perjury that the contents of Parts 3, 4, and 5 of MDOT MBE/DBE Form E are true to the best of my knowledge, information and belief.

Company Name	Signature of Representative
Address	Printed Name and Title
City, State and Zip Code	Date

[1] MBE participation goals and sub-goals apply to State-funded procurements. DBE participation goals apply to federally-funded procurements. Federally-funded contracts do not have sub-goals.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 3 – Identified Items of Work Bidder/Offeror Made Available to MBE/dBE Firms

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

Identify those items of work that the bidder/offeror made available to MBE/DBE Firms. This includes, where appropriate, those items the bidder/offeror identified and determined to subdivide into economically feasible units to facilitate the MBE/DBE participation. For each item listed, show the anticipated percentage of the total contract amount. It is the bidder's/offeror's responsibility to demonstrate that sufficient work to meet the goal was made available to MBE/DBE Firms, and the total percentage of the items of work identified for MBE/DBE participation equals or exceeds the percentage MBE/DBE goal set for the procurement. Note: If the procurement includes a list of bid items identified during the goal setting process as possible items of work for performance by MBE/DBE Firms, the bidder/offeror should make all of those items of work available to MBE/DBE Firms or explain why that item was not made available. If the bidder/offeror selects additional items of work to make available to MBE/DBE Firms, those additional items should also be included below.

Identified Items of Work	Was this work listed in the procurement?	Does bidder/offeror normally self-perform this work?	Was this work made available to MBE/DBE Firms? If no, explain why?
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No

	□ Yes □ No	□ Yes □ No	□ Yes □ No

☐Please check if Additional Sheets are attached.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 4 – Identified MBE/DBE Firms and Record of Solicitations

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

Identify the MBE/DBE Firms solicited to provide quotes for the Identified Items of Work made available for MBE/DBE participation. Include the name of the MBE/DBE Firm solicited, items of work for which bids/quotes were solicited, date and manner of initial and follow-up solicitations, whether the MBE/DBE provided a quote, and whether the MBE/DBE is being used to meet the MBE/DBE participation goal. MBE/DBE Firms used to meet the participation goal must be included on the MBE/DBE Participation Schedule, Form B. Note: If the procurement includes a list of the MBE/DBE Firms identified during the goal setting process as potentially available to perform the items of work, the bidder/offeror should solicit all of those MBE/DBE Firms or explain why a specific MBE/DBE was not solicited. If the bidder/offeror identifies additional MBE/DBE Firms who may be available to perform Identified Items of Work, those additional MBE/DBE Firms should also be included below. Copies of all written solicitations and documentation of follow-up calls to MBE/DBE Firms must be attached to this form. If the bidder/offeror used a Non-MBE/DBE or is self-performing the identified items of work, Part 4 must be completed.

Name of Identified MBE/DBE Firm & MBE Classification	Describe Item of Work Solicited	Initial Solicitation Date & Method	Follow-up Solicitation Date & Method	Details for Follow-up Calls	Quote Rec'd	Quote Used	Reason Quote Rejected
Firm Name: _____ **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____		Date: □ Mail □ Facsimile □ Email	Date: □ Phone □ Mail □ Facsimile □ Email	Time of Call: Spoke With: □ Left Message	□ Yes □ No	□ Yes □ No	□ Used Other MBE/DBE □ Used Non-MBE/DBE □ Self-performing

Name of Identified MBE/DBE Firm & MBE Classification	**Describe Item of Work Solicited**	**Initial Solicitation Date & Method**	**Follow-up Solicitation Date & Method**	**Details for Follow-up Calls**	**Quote Rec'd**	**Quote Used**	**Reason Quote Rejected**
Firm Name: **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____		Date: □ Mail □ Facsimile □ Email	Date: □ Phone □ Mail □ Facsimile □ Email	Time of Call: Spoke With: □ Left Message	□ Yes □ No	□ Yes □ No	□ Used Other MBE/DBE □ Used Non-MBE/DBE □ Self-performing

☐Please check if Additional Sheets are attached.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 5 – Additional Information Regarding Rejected MBE/DBE Quotes

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

This form must be completed if Part 3 indicates that a MBE/DBE quote was rejected because the bidder/offeror is using a Non-MBE/DBE or is self-performing the Identified Items of Work. Provide the Identified Items Work, indicate whether the work will be self-performed or performed by a Non-MBE/DBE, and if applicable, state the name of the Non-MBE/DBE. Also include the names of all MBE/DBE and Non-MBE/DBE Firms that provided a quote and the amount of each quote.

Describe Identified Items of Work Not Being Performed by MBE/DBE (Include spec/section number from bid)	Self-performing or Using Non-MBE/DBE (Provide name)	Amount of Non-MBE/DBE Quote	Name of Other Firms who Provided Quotes & Whether MBE/DBE or Non-MBE/DBE	Amount Quoted	Indicate Reason Why MBE/DBE Quote Rejected & Briefly Explain
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non-MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other

Describe Identified Items of Work Not Being Performed by MBE/DBE (Include spec/section number from bid)	**Self-performing or Using Non-MBE/DBE (Provide name)**	**Amount of Non-MBE/DBE Quote**	**Name of Other Firms who Provided Quotes & Whether MBE/DBE or Non-MBE/DBE**	**Amount Quoted**	**Indicate Reason Why MBE/DBE Quote Rejected & Briefly Explain**
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other

☐Please check if Additional Sheets are attached.

Attachment E. Veteran-Owned Small Business Enterprise (VSBE) Forms

This solicitation does not include a Veteran-Owned Small Business Enterprise goal.

Attachment F. Maryland Living Wage Affidavit of Agreement for Service Contracts

A. This contract is subject to the Living Wage requirements under Md. Code Ann., State Finance and Procurement Article, Title 18, and the regulations proposed by the Commissioner of Labor and Industry (Commissioner). The Living Wage generally applies to a Contractor or subcontractor who performs work on a State contract for services that is valued at $100,000 or more. An employee is subject to the Living Wage if he/she is at least 18 years old or will turn 18 during the duration of the contract; works at least 13 consecutive weeks on the State Contract and spends at least one-half of the employee's time during any work week on the State Contract.

B. The Living Wage Law does not apply to:

(1) A Contractor who:

(a) Has a State contract for services valued at less than $100,000, or

(b) Employs 10 or fewer employees and has a State contract for services valued at less than $500,000.

(2) A subcontractor who:

(a) Performs work on a State contract for services valued at less than $100,000,

(b) Employs 10 or fewer employees and performs work on a State contract for services valued at less than $500,000, or

(c) Performs work for a Contractor not covered by the Living Wage Law as defined in B(1)(b) above, or B (3) or C below.

(3) Service contracts for the following:

(a) Services with a Public Service Company;

(b) Services with a nonprofit organization;

(c) Services with an officer or other entity that is in the Executive Branch of the State government and is authorized by law to enter into a procurement ("Unit"); or

(d) Services between a Unit and a County or Baltimore City.

C. If the Unit responsible for the State contract for services determines that application of the Living Wage would conflict with any applicable Federal program, the Living Wage does not apply to the contract or program.

D. A Contractor must not split or subdivide a State contract for services, pay an employee through a third party, or treat an employee as an independent Contractor or assign work to employees to avoid the imposition of any of the requirements of Md. Code Ann., State Finance and Procurement Article, Title 18.

E. Each Contractor/subcontractor, subject to the Living Wage Law, shall post in a prominent and easily accessible place at the work site(s) of covered employees a notice of the Living Wage Rates, employee rights under the law, and the name, address, and telephone number of the Commissioner.

F. The Commissioner shall adjust the wage rates by the annual average increase or decrease, if any, in the Consumer Price Index for all urban consumers for the Washington/Baltimore metropolitan area, or any successor index, for the previous calendar year, not later than 90 days after the start of each fiscal year. The Commissioner shall publish any adjustments to the wage rates on the

Division of Labor and Industry's website. An employer subject to the Living Wage Law must comply with the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate, required by the Commissioner, automatically upon the effective date of the revised wage rate.

G. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's share of the health insurance premium, as provided in Md. Code Ann., State Finance and Procurement Article, §18-103(c), shall not lower an employee's wage rate below the minimum wage as set in Md. Code Ann., Labor and Employment Article, §3-413. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's share of health insurance premium shall comply with any record reporting requirements established by the Commissioner.

H. A Contractor/subcontractor may reduce the wage rates paid under Md. Code Ann., State Finance and Procurement Article, §18-103(a), by no more than 50 cents of the hourly cost of the employer's contribution to an employee's deferred compensation plan. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's contribution to an employee's deferred compensation plan shall not lower the employee's wage rate below the minimum wage as set in Md. Code Ann., Labor and Employment Article, §3-413.

I. Under Md. Code Ann., State Finance and Procurement Article, Title 18, if the Commissioner determines that the Contractor/subcontractor violated a provision of this title or regulations of the Commissioner, the Contractor/subcontractor shall pay restitution to each affected employee, and the State may assess liquidated damages of $20 per day for each employee paid less than the Living Wage.

J. Information pertaining to reporting obligations may be found by going to the Division of Labor and Industry website http://www.dllr.state.md.us/labor/prev/livingwage.shmtl and clicking on Living Wage for State Service Contracts.

F-1 Maryland Living Wage Requirements Affidavit of Agreement

Contract No. J02B8400024

Name of Contractor:

Address:

If the Contract Is Exempt from the Living Wage Law

The Undersigned, being an authorized representative of the above named Contractor, hereby affirms that the Contract is exempt from Maryland's Living Wage Law for the following reasons (check all that apply):

☐ Offeror is a nonprofit organization

☐ Offeror is a public service company

☐ Offeror employs 10 or fewer employees and the proposed contract value is less than $500,000

☐ Offeror employs more than 10 employees and the proposed contract value is less than $100,000

If the Contract Is a Living Wage Contract

A. The Undersigned, being an authorized representative of the above-named Contractor, hereby affirms its commitment to comply with Title 18, State Finance and Procurement Article, Annotated Code of Maryland and, if required, submit all payroll reports to the Commissioner of Labor and Industry with regard to the above stated contract. The Offeror agrees to pay covered employees who are subject to living wage at least the living wage rate in effect at the time service is provided for hours spent on State contract activities, and ensure that its subcontractors who are not exempt also pay the required living wage rate to their covered employees who are subject to the living wage for hours spent on a State contract for services. The Contractor agrees to comply with, and ensure its subcontractors comply with, the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate established by the Commissioner of Labor and Industry, automatically upon the effective date of the revised wage rate.

B. _____ (initial here if applicable) The Offeror affirms it has no covered employees for the following reasons: (check all that apply):

☐ The employee(s) proposed to work on the contract will spend less than one-half of the employee's time during any work week on the contract

☐ The employee(s) proposed to work on the contract is 17 years of age or younger during the duration of the contract; or

☐ The employee(s) proposed to work on the contract will work less than 13 consecutive weeks on the State contract.

The Commissioner of Labor and Industry reserves the right to request payroll records and other data that the Commissioner deems sufficient to confirm these affirmations at any time.

Name of Authorized Representative:

Signature of Authorized Representative : _____Date: _____

Title:

Witness Name (Typed or Printed) _____

Witness Signature: _____ Date: _____

SUBMIT THIS AFFIDAVIT WITH PROPOSAL

Attachment G. Federal Funds Attachments

This solicitation does not include a Federal Funds Attachment.

Attachment H. Conflict of Interest Affidavit and Disclosure

Reference COMAR 21.05.08.08

A. "Conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the State, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

B. "Person" has the meaning stated in COMAR 21.01.02.01B (64) and includes a bidder, offeror, contractor, consultant, or subcontractor or sub-consultant at any tier, and also includes an employee or agent of any of them if the employee or agent has or will have the authority to control or supervise all or a portion of the work for which a bid or offer is made.

C. The bidder or offeror warrants that, except as disclosed in §D, below, there are no relevant facts or circumstances now giving rise or which could, in the future, give rise to a conflict of interest.

D. The following facts or circumstances give rise or could in the future give rise to a conflict of interest (explain in detail—attach additional sheets if necessary):

E. The bidder or offeror agrees that if an actual or potential conflict of interest arises after the date of this affidavit, the bidder or offeror shall immediately make a full disclosure in writing to the procurement officer of all relevant facts and circumstances. This disclosure shall include a description of actions which the bidder or offeror has taken and proposes to take to avoid, mitigate, or neutralize the actual or potential conflict of interest. If the contract has been awarded and performance of the contract has begun, the Contractor shall continue performance until notified by the procurement officer of any contrary action to be taken.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By: _____

(Authorized Representative and Affiant

Attachment I. Non-Disclosure Agreement (TO Contractor)

THIS NON-DISCLOSURE AGREEMENT ("Agreement") is made by and between the State of Maryland (the "State"), acting by and through (Maryland Department of Transportation State Highway Administration) (the "Agency"), and _____ (the "TO Contractor").

RECITALS

WHEREAS, the TO Contractor has been awarded a contract (the "TO Agreement") following the solicitation for SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP Solicitation # J02B8400024; and

WHEREAS, in order for the TO Contractor to perform the work required under the TO Agreement, it will be necessary for the State at times to provide the TO Contractor and the TO Contractor's employees, agents, and subcontractors (collectively the "TO Contractor's Personnel") with access to certain information the State deems confidential information (the "Confidential Information").

NOW, THEREFORE, in consideration of being given access to the Confidential Information in connection with the solicitation and the TO Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1. Regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such, "Confidential Information" means (1) any and all information provided by or made available by the State to the TO Contractor in connection with the TO Agreement and (2) any and all personally identifiable information (PII) (including but not limited to personal information as defined in Md. Ann. Code, General Provisions §4-101(h)) and protected health information (PHI) that is provided by a person or entity to the TO Contractor in connection with this TO Agreement. Confidential Information includes, by way of example only, information that the TO Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the TO Agreement.
2. The TO Contractor shall not, without the State's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information except for the sole and exclusive purpose of performing under the TO Agreement. The TO Contractor shall limit access to the Confidential Information to the TO Contractor's Personnel who have a demonstrable need to know such Confidential Information in order to perform under TO Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. The names of the TO Contractor's Personnel are attached hereto and made a part hereof as **Attachment I-2**. TO Contractor shall update **Attachment I-2** by adding additional names (whether TO Contractor's Personnel or a subcontractor's personnel) as needed, from time to time.
3. If the TO Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the TO Contractor's performance of the TO Agreement or will otherwise have a role in performing any aspect of the TO Agreement, the TO Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.
4. The TO Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, adopt or establish operating procedures and physical security measures, and take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties and to prevent all or any portion of the Confidential Information from falling

into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.

5. The TO Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the TO Contractor's Personnel or the TO Contractor's former Personnel. TO Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).
6. The TO Contractor shall, at its own expense, return to the Agency all Confidential Information in its care, custody, control or possession upon request of the Agency or on termination of the TO Agreement.
7. A breach of this Agreement by the TO Contractor or the TO Contractor's Personnel shall constitute a breach of the TO Agreement between the TO Contractor and the State.
8. TO Contractor acknowledges that any failure by the TO Contractor or the TO Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the TO Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The TO Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and seek damages from the TO Contractor and the TO Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the TO Contractor or any of the TO Contractor's Personnel to comply with the requirements of this Agreement, the TO Contractor shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and costs.
9. TO Contractor and each of the TO Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement, in no event less restrictive than as set forth in this Agreement, and the TO Contractor shall provide originals of such executed Agreements to the State.
10. The parties further agree that:
    a. This Agreement shall be governed by the laws of the State of Maryland;
    b. The rights and obligations of the TO Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State;
    c. The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information;
    d. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement;
    e. Signatures exchanged by facsimile are effective for all purposes hereunder to the same extent as original signatures;
    f. The Recitals are not merely prefatory but are an integral part hereof; and
    g. The effective date of this Agreement shall be the same as the NTP date of the TO Agreement entered into by the parties.

IN WITNESS WHEREOF, the parties have, by their duly authorized representatives, executed this Agreement as of the day and year first above written.

TO Contractor:	SHA
By: (seal)	By:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

I-2 NON-DISCLOSURE AGREEMENT

LIST OF CONTRACTOR'S EMPLOYEES AND AGENTS WHO WILL BE GIVEN ACCESS TO THE CONFIDENTIAL INFORMATION

Printed Name and Address of Individual/Agent	Employee (E) or Agent (A)	Signature	Date

I-3 NON-DISCLOSURE AGREEMENT

CERTIFICATION TO ACCOMPANY RETURN OR DELETION OF CONFIDENTIAL INFORMATION

I AFFIRM THAT:

To the best of my knowledge, information, and belief, and upon due inquiry, I hereby certify that: (i) all Confidential Information which is the subject matter of that certain Non-Disclosure Agreement by and between the State of Maryland and _____ ("TO Contractor") dated _____, 20_____ ("Agreement") is attached hereto and is hereby returned to the State in accordance with the terms and conditions of the Agreement; and (ii) I am legally authorized to bind the TO Contractor to this affirmation. Any and all Confidential Information that was stored electronically by me has been permanently deleted from all of my systems or electronic storage devices where such Confidential Information may have been stored.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF, HAVING MADE DUE INQUIRY.

DATE: _____

NAME OF TO CONTRACTOR: _____

BY: _____
(Signature)

TITLE: _____

Attachment J. HIPAA Business Associate Agreement

This solicitation does not require a HIPAA Business Associate Agreement.

Attachment K. Mercury Affidavit

This solicitation does not include the procurement of products known to likely include mercury as a component.

Attachment L. Location of the Performance of Services Disclosure

(submit with Proposal)

Pursuant to Md. Ann. Code, State Finance and Procurement Article, § 12-111, and in conjunction with the Proposal submitted in response to Solicitation No. J02B8400024, the following disclosures are hereby made:

1. At the time of Proposal submission, the Offeror and/or its proposed subcontractors:

___have plans

___have no plans

to perform any services required under the TO Agreement outside of the United States.

2. If services required under the contract are anticipated to be performed outside the United States by either the Offeror or its proposed subcontractors, the Offeror shall answer the following (attach additional pages if necessary):

a. Location(s) services will be performed:

_____
_____
_____

b. Reasons why it is necessary or advantageous to perform services outside the United States:

_____
_____
_____
_____
_____

The undersigned, being an authorized representative of the Offeror, hereby affirms that the contents of this disclosure are true to the best of my knowledge, information, and belief.

Date: _____

Offeror Name:

By: _____

Name:

Title:

Please be advised that the Agency may contract for services provided outside of the United States if: the services are not available in the United States; the price of services in the United States exceeds by an unreasonable amount the price of services provided outside the United States; or the quality of services in the United States is substantially less than the quality of comparably priced services provided outside the United States.

Attachment M. Task Order

CATS+ TORFP# J02B8400024 OF
MASTER CONTRACT #060B2490023

This Task Order Agreement ("TO Agreement") is made this day of Month, 2018 by and between _____ (TO Contractor) and the STATE OF MARYLAND, Maryland Department of Transportation State Highway Administration (SHA or the "Agency").

IN CONSIDERATION of the mutual promises and the covenants herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. In this TO Agreement, the following words have the meanings indicated:

   a. "Agency" means Maryland Department of Transportation State Highway Administration, as identified in the CATS+ TORFP # J02B8400024.

   b. "CATS+ TORFP" means the Task Order Request for Proposals # J02B8400024, dated MONTH DAY, YEAR, including any addenda and amendments.

   c. "Master Contract" means the CATS+ Master Contract between the Maryland Department of Information Technology and TO Contractor.

   d. "TO Procurement Officer" means <<TO Procurement Officer>>. The Agency may change the TO Procurement Officer at any time by written notice.

   e. "TO Agreement" means this signed TO Agreement between SHA and TO Contractor.

   f. "TO Contractor" means the CATS+ Master Contractor awarded this TO Agreement, whose principal business address is _____.

   g. "TO Manager" means Mark W Harrison. The Agency may change the TO Manager at any time by written notice to the TO Contractor.

   h. "TO Technical Proposal" means the TO Contractor's technical response to the CATS+ TORFP dated date of TO Technical Proposal.

   i. "TO Financial Proposal" means the TO Contractor's financial response to the CATS+ TORFP dated date of TO Financial Proposal.

   j. "TO Proposal" collectively refers to the TO Technical Proposal and TO Financial Proposal.

2. Scope of Work

2.1 This TO Agreement incorporates all of the terms and conditions of the Master Contract and shall not in any way amend, conflict with or supersede the Master Contract.

2.2 The TO Contractor shall, in full satisfaction of the specific requirements of this TO Agreement, provide the services set forth in Section 3 of the CATS+ TORFP. These services shall be provided in accordance with the Master Contract, this TO Agreement, and the following Exhibits, which are attached and incorporated herein by reference. If there is any conflict among the Master Contract, this TO Agreement, and these Exhibits, the terms of the Master Contract shall govern. If there is any conflict between this TO Agreement and any of these Exhibits, the following order of precedence shall determine the prevailing provision:

The TO Agreement,

Exhibit A – CATS+ TORFP

Exhibit B – TO Technical Proposal

Exhibit C – TO Financial Proposal

2.3 The TO Procurement Officer may, at any time, by written order, make changes in the work within the general scope of the TO Agreement. No other order, statement or conduct of the TO Procurement Officer or any other person shall be treated as a change or entitle the TO Contractor to an equitable adjustment under this Section. Except as otherwise provided in this TO Agreement, if any change under this Section causes an increase or decrease in the TO Contractor's cost of, or the time required for, the performance of any part of the work, whether or not changed by the order, an equitable adjustment in the TO Agreement price shall be made and the TO Agreement modified in writing accordingly. The TO Contractor must assert in writing its right to an adjustment under this Section within thirty (30) days of receipt of written change order and shall include a written statement setting forth the nature and cost of such claim. No claim by the TO Contractor shall be allowed if asserted after final payment under this TO Agreement. Failure to agree to an adjustment under this Section shall be a dispute under the Disputes clause of the Master Contract. Nothing in this Section shall excuse the TO Contractor from proceeding with the TO Agreement as changed.

3. Time for Performance

This TO Agreement is effective as of the date of Notice to Proceed (NTP). Unless terminated earlier as provided in the Master Contract the term of this TO Agreement is for a period of 5 years commencing on the NTP Date and terminating on the 5th anniversary thereof.

4. Consideration and Payment

4.1 The consideration to be paid the TO Contractor shall be done so in accordance with the CATS+ TORFP and shall not exceed $_____. Any work performed by the TO Contractor in excess of the not-to-exceed ceiling amount of the TO Agreement without the prior written approval of the TO Manager is at the TO Contractor's risk of non-payment.

4.2 Payments to the TO Contractor shall be made as outlined Section 3 of the CATS+ TORFP, but no later than thirty (30) days after the Agency's receipt of a proper invoice for services provided by the TO Contractor, acceptance by the Agency of services provided by the TO Contractor, and pursuant to the conditions outlined in Section 4 of this Agreement.

4.3 Each invoice for services rendered must include the TO Contractor's Federal Tax Identification Number which is _____. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1, of the State Finance and Procurement Article, Annotated Code of Maryland, as from time-to-time amended, are prohibited. Invoices must be submitted to the Agency TO Manager unless otherwise specified herein.

4.4 In addition to any other available remedies, if, in the opinion of the TO Procurement Officer, the TO Contractor fails to perform in a satisfactory and timely manner, the TO Procurement Officer may refuse or limit approval of any invoice for payment, and may cause payments to the TO Contractor to be reduced or withheld until such time as the TO Contractor meets performance standards as established by the TO Procurement Officer.

SIGNATURES ON NEXT PAGE

IN WITNESS THEREOF, the parties have executed this TO Agreement as of the date hereinabove set forth.

TO Contractor Name

_____ _____

By: Type or Print TO Contractor POC Date

Witness: _____

STATE OF MARYLAND, SHA

_____ _____

By: Peggy Tischler, TO Procurement Officer Date

Witness: _____

Approved for form and legal sufficiency this _____ day of _____ 20___.

_____

Assistant Attorney General

Attachment N. Certification Regarding Investments in Iran

Authority: State Finance & Procurement, §§17-701 – 17-707, Annotated Code of Maryland [Chapter 447, Laws of 2012.]

List: The Investment Activities in Iran list identifies companies that the Board of Public Works has found to engage in investment activities in Iran; those companies may not participate in procurements with a public body in the State. "Engaging in investment activities in Iran" means:

A. Providing goods or services of at least $20 million in the energy sector of Iran; or

B. For financial institutions, extending credit of at least $20 million to another person for at least 45 days if the person is on the Investment Activities In Iran list and will use the credit to provide goods or services in the energy of Iran.

The Investment Activities in Iran list is located at: www.bpw.state.md.us

Rule: A company listed on the Investment Activities In Iran list is ineligible to bid on, submit a proposal for, or renew a contract for goods and services with a State Agency or any public body of the State. Also ineligible are any parent, successor, subunit, direct or indirect subsidiary of, or any entity under common ownership or control of, any listed company.

NOTE: This law applies only to new contracts and to contract renewals. The law does not require an Agency to terminate an existing contract with a listed company.

CERTIFICATION REGARDING INVESTMENTS IN IRAN

The undersigned certifies that, in accordance with State Finance & Procurement Article, §17-705:

(i) it is not identified on the list created by the Board of Public Works as a person engaging in investment activities in Iran as described in §17-702 of State Finance & Procurement; and

(ii) it is not engaging in investment activities in Iran as described in State Finance & Procurement Article, §17-702.

The undersigned is unable make the above certification regarding its investment activities in Iran due to the following activities:

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Date: _____ Title: _____

Witness Name (Typed or Printed): _____

Witness Signature and Date: _____

Appendix 1. – Abbreviations and Definitions

For purposes of this TORFP, the following abbreviations or terms have the meanings indicated below:

A. Application Program Interface (API) - Code that allows two software programs to communicate with each other
B. Access - The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource
C. Business Day(s) – The official working days of the week to include Monday through Friday. Official working days excluding State Holidays (see definition of "Normal State Business Hours" below).
D. COMAR – Code of Maryland Regulations available on-line at http://www.dsd.state.md.us/COMAR/ComarHome.html.
E. Data Breach – The unauthorized acquisition, use, modification or disclosure of State data, or other Sensitive Data
F. Effective Date – Is the NTP Date, the date of mutual TO Agreement execution by the parties
G. Enterprise License Agreement (ELA) – An agreement to license the entire population of an entity (employees, on-site contractors, off-site contractors) accessing a software or service for a specified period of time for a specified value.
H. Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
I. Information Technology (IT) – All electronic information-processing hardware and software, including: (a) maintenance; (b) telecommunications; and (c) associated consulting services
J. Key Personnel – All TO Contractor Personnel identified in the solicitation as such that are essential to the work being performed under the Task Order. See TORFP **Section 3.10.5**.
K. Local Time – Time in the Eastern Time Zone as observed by the State of Maryland. Unless otherwise specified, all stated times shall be Local Time, even if not expressly designated as such.
L. Maryland Department of Transportation State Highway Administration or (SHA or the "Agency")
M. Minority Business Enterprise (MBE) – Any legal entity certified as defined at COMAR 21.01.02.01B (54) which is certified by the Maryland Department of Transportation under COMAR 21.11.03.
N. Normal State Business Hours - Normal State business hours are 8:00 a.m. – 5:00 p.m. Monday through Friday except State Holidays, which can be found at: www.dbm.maryland.gov – keyword: State Holidays.
O. Notice to Proceed (NTP) – A written notice from the TO Manager that work under the Task Order, project or Work Order (as applicable) is to begin as of a specified date. The NTP Date is the start date of work under the Task Order, project or Work Order. Additional NTPs may be issued by the TO Manager regarding the start date for any service included within this solicitation with a delayed or non-specified implementation date.

P. NTP Date – The date specified in a NTP for work on Task Order, project or Work Order to begin.
Q. Offeror – A Master Contractor that submits a Proposal in response to this TORFP.
R. Personally Identifiable Information (PII) – Any information about an individual maintained by the State, including (1) any information that can be used to distinguish or trace an individual identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
S. Protected Health Information (PHI) – Information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
T. Security Incident – A violation or imminent threat of violation of computer security policies, Security Measures, acceptable use policies, or standard security practices. "Imminent threat of violation" is a situation in which the organization has a factual basis for believing that a specific incident is about to occur.
U. Security or Security Measures – The technology, policy and procedures that a) protects and b) controls access to networks, systems, and data
V. Sensitive Data - Means PII;PHI; other proprietary or confidential data as defined by the State, including but not limited to "personal information" under Md. Code Ann., Commercial Law § 14-3501(d) and Md. Code Ann., St. Govt. § 10-1301(c) and information not subject to disclosure under the Public Information Act, Title 4 of the General Provisions Article; and .information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information
W. Software - The object code version of computer programs licensed pursuant to this TO Agreement. Embedded code, firmware, internal code, microcode, and any other term referring to software that is necessary for proper operation is included in this definition of Software. Software includes all prior, current, and future versions of the Software and all maintenance updates and error corrections. Software also includes any upgrades, updates, bug fixes or modified versions or backup copies of the Software licensed to the State by TO Contractor or an authorized distributor.
X. Solution - All Software, deliverables, services and activities necessary to fully provide and support the TORFP scope of work. This definition of Solution includes all System Documentation developed as a result of this TO Agreement. Also included are all Upgrades, patches, break/fix activities, enhancements and general maintenance and support of the Solution and its infrastructure.
Y. State – The State of Maryland.
Z. Source Code – Executable instructions for Software in its high level, human readable form which are in turn interpreted, parsed and/or compiled to be executed as part of a computing system.

AA. System Availability – The period of time the Solution works as required excluding non-operational periods associated with planned maintenance.

BB. System Documentation – Those materials necessary to wholly reproduce and fully operate the most current deployed version of the Solution in a manner equivalent to the original Solution including, but not limited to:

1) Source Code: this includes source code created by the TO Contractor or subcontractor(s) and source code that is leveraged or extended by the TO Contractor for use in the Task Order.
2) All associated rules, reports, forms, templates, scripts, data dictionaries and database functionality.
3) All associated configuration file details needed to duplicate the run time environment as deployed in the current deployed version of the system.
4) All associated design details, flow charts, algorithms, processes, formulas, pseudo-code, procedures, instructions, help files, programmer's notes and other documentation.
5) A complete list of Third Party, open source, or commercial software components and detailed configuration notes for each component necessary to reproduce the system (e.g., operating system, relational database, and rules engine software).
6) All associated user instructions and/or training materials for business users and technical staff, including maintenance manuals, administrative guides and user how-to guides.
7) Operating procedures

CC. Task Order (TO) – The scope of work described in this TORFP.

DD. TO Agreement - The contract awarded to the successful Offeror pursuant to this Task Order Request for Proposals, the form of which is attached to this TORFP as **Attachment M.**

EE. TO Contractor Personnel - Employees and agents and subcontractor employees and agents performing work at the direction of the TO Contractor under the terms of the Task Order awarded from this TORFP.

FF. TO Proposal – As appropriate, either or both of an Offeror's TO Technical or TO Financial Proposal.

GG. Technical Safeguards – The technology and the policy and procedures for its use that protect State Data and control access to it.

HH. Third Party Software – Software and supporting documentation that:

8) are owned by a third party, not by the State, the TO Contractor, or a subcontractor,
9) are included in, or necessary or helpful to the operation, maintenance, support or modification of the Solution; and
10) were specifically identified and listed as Third Party Software in the Proposal.

II. Total Proposal Price - The Offeror's total proposed price for services in response to this solicitation, included in the TO Financial Proposal with **Attachment B** – TO Financial Proposal Form, and used in the financial evaluation of Proposals (see TORFP **Section 5.5**).

JJ. Veteran-owned Small Business Enterprise (VSBE) – A business that is verified by the Center for Verification and Evaluation (CVE) of the United States Department of

Veterans Affairs as a veteran-owned small business. See Code of Maryland Regulations (COMAR) 21.11.13.

KK. Work Order– A subset of work authorized by the TO Manager performed under the general scope of this TORFP, which is defined in advance of TO Contractor fulfillment, and which may not require a TO Agreement modification. Except as otherwise provided, any reference to the Task Order shall be deemed to include reference to a Work Order.

Appendix 2. – Offeror Information Sheet

Offeror	
Company Name	
Street Address	
City, State, Zip Code	
TO Contractor Federal Employer Identification Number (FEIN)	
TO Contractor eMM ID number	As of the date of Proposal submission, are you registered to do business with the state of Maryland?
SBE / MBE/ VSBE Certification	
SBE	Number: Expiration Date:
VSBE	Number: Expiration Date:
MBE	Number: Expiration Date: Categories to be applied to this solicitation (dual certified firms must choose only one category).
Offeror Primary Contact	
Name	
Title	
Office Telephone number (with area code)	
Cell Telephone number (with area code)	
e-mail address	
Authorized Offer Signatory	
Name	
Title	
Office Telephone number (with area code)	
Cell Telephone number (with area code)	
e-mail address	

Appendix 3. - Labor Classification Personnel Resume Summary

INSTRUCTIONS:

1. For each person proposed, complete one Labor Category Personnel Resume Summary to document how the proposed person meets each of the minimum requirements.

   For example: If you propose John Smith, who is your subcontractor, and you believe he meets the requirements of the Group Facilitator, you will complete the top section of the form by entering John Smith's name and the subcontractor's company name. You will then complete the right side of the Group Facilitator form documenting how the individual meets each of the requirements. Where there is a time requirement such as three months experience, you must provide the dates from and to showing an amount of time that equals or exceeds mandatory time requirement; in this case, three months.

2. Additional information may be attached to each Labor Category Personnel Resume Summary that may assist a full and complete understanding of the individual being proposed.

3. For this TORFP,

   A. Master Contractors shall comply with all personnel requirements defined under the Master Contract RFP 060B2490023.
   B. Master Contractors shall propose the CATS+ Labor Category that best fits each proposed resource. A Master Contractor may only propose against labor categories in the Master Contractor's CATS+ Master Contract Financial Proposal.
   C. A Master Contractor's entire TO Technical Proposal will be deemed not susceptible for award if any of the following occurs:
      1) Failure to follow these instructions.
      2) Failure to propose a resource for each job title or labor category identified in the TORFP as a required submission.
      3) Failure of any proposed resource to meet minimum requirements as listed in this TORFP and in the CATS+ Master Contract.
      4) Placing content on the **Minimum Qualifications Summary** that is not also on the **Personnel Resume Summary**. *The function of the **Minimum Qualifications Summary** is to aid the agency to make a minimum qualification determination. Information on the **Minimum Qualification Summary** must correspond with information on the **Personnel Resume Summary** and shall not contain additional content not found on the other form.*

4. Complete and sign the **Minimum Qualifications Summary (Appendix 3A)** and the **Personnel Resume Form (Appendix 3B)** for each resource proposed. Alternate resume formats are not allowed.

   a. The **Minimum Qualifications Summary** demonstrates the proposed resource meets minimum qualifications for the labor category, as defined in the CATS+ RFP Section 2.10, and any additional minimum requirements stated in this TORFP. For each minimum qualification, indicate the location on the **Personnel Resume Form (Appendix 3B)** demonstrating meeting this requirement.

      Only include the experience relevant to meeting a particular minimum qualification. Every skill must be linked to specific work experience and/or education. The **Minimum**

Qualification Summary shall not contain content that cannot be correlated to the **Personnel Resume Summary**.

Every experience listed on the **Minimum Qualifications Resume Summary** must be explicitly listed with start and stop dates. Where there is a time requirement such as three months' experience, you must provide the dates from and to showing an amount of time that equals or exceeds the mandatory time requirement; in this case, three months. Note: Overlapping time periods shall only count once against a specific minimum qualification (i.e., a minimum qualification may not be met by listing two examples occurring during the same time period.).

b. The **Personnel Resume Form** provides resumes in a standard format. Additional information may be attached to each **Personnel Resume Summary** if it aids a full and complete understanding of the individual proposed.

3A MINIMUM QUALIFICATIONS SUMMARY

Appendix 3 - Labor Classification Key Personnel Resume Summary Form

CATS+ TORFP # J02B8400024

All content on this form must also be on the Personnel Resume Form.
ONLY include information on this summary that supports meeting a minimum qualification.

Proposed Key Personnel:	Master Contractor:			CATS+ Labor Category:	
Education: (Insert the education requirements for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP	Institution/Address:			Degree or Certification: Field of Study:	Year Completed:
Generalized Experience: (Insert the generalized experience description for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP)	Start	End	Company/Job Title	Relevant Work Experience	
Specialized Experience: (Insert the specialized experience description for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP)	Start	End	Company/Job Title	Relevant Work Experience	
TORFP Additional Requirements (Insert, if applicable, the additional requirements from Section 1.1 and 2.10 of the CATS+ RFP)					

The information provided on this form for this labor category is true and correct to the best of my knowledge:

Master Contractor Representative:	Proposed Key Personnel:
Signature	Signature
Printed Name:	Printed Name
Date	Date

Sign each Form

3B. Labor Classification Personnel Resume Summary

TORFP # J02B8400024

Instructions: Enter resume information in the fields below; do not submit other resume formats. Submit one resume for each proposed resource

Candidate Name:	
TO Contractor:	(offerorCompanyName)

Education / Training

Institution Name / City / State	Degree / Certification	Year Completed	Field Of Study
<add lines as needed>			

Relevant Work Experience

Describe work experience relevant to the Duties / Responsibilities and Minimum Qualifications described in the TORFP. Starts with the most recent experience first; do not include non-relevant experience.

[Organization] [Title / Role] [Period of Employment / Work] [Location] [Contact Person (Optional if current employer)]	Description of Work…
[Organization] [Title / Role] [Period of Employment / Work] [Location] [Contact Person]	Description of Work…
<add lines as needed>	

Employment History

List employment history, starting with the most recent employment first

Start and End Dates	Job Title or Position	Organization Name	Reason for Leaving
<add lines as needed>			

Personnel Resume Summary (Continued)

*"Candidate Relevant Experience" section must be filled out. Do not enter "see resume" as a response.

References

List persons the State may contact as employment references

Reference Name	Job Title or Position	Organization Name	Telephone / E-mail
<add lines as needed>			

Proposed Individual's Name/Company Name:	How does the proposed individual meet each requirement?
LABOR CATEGORY TITLE:	*Offeror to Enter the Labor Category Name*
Requirement (See Section 2.10 of the CATS+ Master Contract)	Candidate Relevant Experience *
Education: [Insert the education description from Section 2.10 of the CAST+ Master Contract for the applicable labor category]	Education:
Experience: [Insert the experience description from Section <<x.x>>for the applicable labor category]	Experience:
Duties: [Insert the duties description from Section <<x.x>>for the applicable labor category]	Duties:

The information provided on this form for this labor category is true and correct to the best of my knowledge:

TO Contractor Representative:	Proposed Individual:
Signature	Signature
Printed Name:	Printed Name
Date	Date

Sign each Form

Appendix 4 – Criminal Background Check Affidavit

AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the _____(Title)_____ and the duly authorized representative of ___(Master Contractor)_____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

I hereby affirm that ____ (Master Contractor) _____ has complied with Section 2.4, Security Requirements of the Department of Information Technology's Consulting Technical Services Master Contract Number 060B2490023 (CATS+) hereto as Exhibit A.

I hereby affirm that the ____ (Master Contractor)_____ has provided Maryland Transportation Authority with a summary of the security clearance results for all of the candidates that will be working on Task Order MICROSOFT DYNAMICS SL SOFTWARE TECHNICAL AND USER SUPPORT J02B8400024 and all of these candidates have successfully passed all of the background checks required under Section 2.4.3.2 of the CATS + Master Contract. Master Contractors hereby agrees to provide security clearance results for any additional candidates at least seven (7) days prior to the date the candidate commences work on this Task Order.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

_____

Master Contractor

_____

Typed Name

_____

Signature

_____

Date

This for is due within 30 days of notice of award

Appendix 5 - Maryland Department of Transportation Information Security Plan

See separate Attachment

Appendix 6 Weekly TO Contractor Personnel Status Report

Weekly Status Report

Week Starting: <<week starts on a Monday>>	**Date: <<date prepared mm/dd/yyyy>>**
Report Prepared by: <<TO Contractor Personnel>>	**Task Number: J02B3400049**
TO Contractor: <<name of the TO Contractor>>	
Task Name: SHA Business Application Portfolio Business Services Task Order	

Name	Labor Category	Hours Expended for the
<<TO Contractor Personnel>>	<<labor category name associated with TO Contractor Personnel>>	<<##.#>>

ACTIVITIES COMPLETED:

<<Activity 1 Name>> ***(##.# Hours)***

- <<activity task 1>>
- <<activity task 2>>
- <<activity task 3>>
- <<activity task 4>>

Administrative ***(##.# Hour)***

- <<activity task 1>>
- <<activity task 2>>
- <<activity task 3>>

ACTIVITIES IN PROGRESS:

- <<Activity 1 Name>>

NEXT WEEK PLANNED ACTIVITIES

- <<activity 1 description>>

ACTIVITIES ON HOLD/ISSUES:

- <<Activity/Issue>>

ACTIVITIES REQUIRING OVERTIME AND TIME USED:

Date	Hours	Comments

ACTION ITEMS:

Item	Status	Comments

Appendix 7 - CERTIFICATION REGARDING DISCRIMINATORY BOYCOTTS OF ISRAEL

Authority: Executive Order 01.01.2017.25 (issued October 23, 2017)

☐ The undersigned offeror hereby certifies and agrees that the following information is correct:

In preparing its proposal on this project, the offeror has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not, in the solicitation, selection, or commercial treatment of any subcontractor, vendor, or supplier, refused to transact or terminated business activities, or taken other actions intended to limit commercial relations, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel and its territories. The offeror also has not retaliated against any person or other entity for reporting such refusal, termination, or commercially limiting actions. Without limiting any other provision of the solicitation for this project, it is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the proposal submitted by the offeror on this project, and terminate any contract awarded based on the bid.

☐ The undersigned is unable make the above certification regarding boycotts of Israel due to the following activities:

_____

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS CERTIFICATION ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Date: _____ Title:_____

MARYLAND DEPARTMENT OF TRANSPORTATION

April 24, 2018

Office of Procurement
TORFP: J028B8400024
SHA APPLICATION PORTFOLIO BUSINESS SERVICES

This Amendment is issued to Extend the Due Date, Answer Questions submitted by vendors, clarify, add to, delete from, correct and/or change the TORFP documents to the extent indicated and is hereby made a part of the above named TORFP and on which the contract will be based. All information contained herein is binding on all offerors who respond to this TORFP. Specific parts of the TORFP have been amended.

The Due Date and Time for Technical Proposals for the above Named TORFP has been extended from Monday, May 7, 2018 to Friday, May 11,2018 @ 2:00pm (EST)

Reference TORFP Documents:

The TORFP Document has been revised. Please DISCARD previous copies of the TORFP originally sent out on April 4, 2018. REPLACE WITH the TORFP as amended April 24, 201. All changes to the TORFP are highlighted.

The changes can be found in:
Key Information Sheet
Table of Contents
Section 2.1.1
Section 3.12.2
Replace: Revised – Attachment B - Form B-1 Financial Proposal Form
Delete: page 108, "APPENDIX 3 – Labor Classifications Key Personnel Resume Summary Form"
Add: Appendix – "3A Minimum Qualification Summary" form

SEE ATTACHED:

Question and Answers

MARYLAND DEPARTMENT OF TRANSPORTATION

April 24, 2018

Question 1: Can you tell me who the incumbent is and if there is an option year on their contract?
ANSWER 1: The incumbent is CNSI. There is no option year(s) on the current contract.

Question 2: Section 1.1 shows only 3 resources required but later it was expecting 4 key personnel. Please clarify.
ANSWER 2: Section 1.1 refers to the three (3) positions that the Offeror must specify a Labor Category for, for Key Personnel. Section 3.10.5 - Key Personnel Identified, lists the number of key personnel per position.

Question 3: There are two locations provided to perform work. At which one will the initial 4 resources will be working?
ANSWER 3: At the location of: 7491 Connelly Drive, Hanover MD. 21076, SHA will require the following key personnel:
One (1) Senior .Net Programmer (reference section 1.1.1)

At the location of: 707 N. Calvert Street, Baltimore MD. 21202, SHA will require the following key personnel:
One (1) Senior .Net Programmer (reference section 1.1.1)
One (1) Senior SalesForce.com Programmer (reference section 1.1.2)
One (1) Senior PowerBuilder Programmer (reference section 1.1.3)

Question 4: Are there any incumbent for any of the openings?
ANSWER 4: See answer to Question 1

Question 5: Please let us know labor categories for all six resources (current and future)
ANSWER 5 The Cats+ Labor Categories are to be proposed by the Master Contractor. Please reference Attachment B, B-1 FINANCIAL PROPOSAL FORM: "ALL LABOR CATEGORIES ARE TO BE SELECTED FROM THE CATS+ MASTER CONTRACT SECTION 2.10"

Question 6: If an MBE woman-owned company submits as the prime, can they then count themselves for the entire percentage (%) of an MBE sub-goal that they qualify for? For instance, if a prime company is woman owned, then can they count for the entire woman-owned MBE portion of the woman-owned sub-goal participation? Is that correct? If so, would we just put ourselves down on the MBE forms?
ANSWER 6: Yes, this is correct. If an MBE woman-owned company submits as the prime, they can then count themselves for the entire percentage (100%) of a woman-owned

MBE sub-goal. Yes, you would put your company down on the MBE forms as the Prime and for the MBE sub-goal you qualify for. MBE Primes may also count themselves toward 50% of the overall contract goal.

Question 7: Are there any incumbents (existing resource/vendor) for this position? If Yes, how many?

ANSWER 7: See Answer to Question 1 for name of incumbent. Currently the incumbent has 18 resources working under the current contact.

Question 8: Do we need to identify all the minority partners in the proposal or can we provide details after the award?

ANSWER 8: All MBE subcontractors fulfilling the MBE and MBE sub-goals must be identified in the MDOT MBE Form submission included in the Technical Proposal. Also, per Section 5.4.2 E – Subcontractors, states: "Identify all proposed Subcontractors, including MBEs, and their roles in the performance of the scope of work hereunder." (also see 5.4.2 D 1, and 5.4.2 G)

Question 9: Do the Key Personnel submitted for the proposal have to be on our payroll at the time of proposal submission or is it sufficient for us to obtain a letter of intent from the key proposal to join us at the time of the award?

ANSWER 9: Key personnel do not have to be on a company's payroll at time of proposal submission. However, if a substitution of key personnel either prior to and 30 days after task order execution becomes necessary subcontractors, temporary staff or 1099 contractors do not qualify, and could find the offeror eliminated from further consideration. Please see Sections 3.11.2 A and B for further information.

Question 10: Since this is a staff augmentation RFP, and no technical solution (other than providing the requested staff) is required from the vendor, is the proposal going to be evaluated mainly on the quality of the resumes of the key personnel?

ANSWER 10: Please see Section 6.2 for the specific Technical Proposal Evaluation Criteria information, including Oral Presentations (section 4.5). Also see Section 6.4 - Selection Procedures, and more specifically sub-sections A and B.

Question 11: Can the state please provide a list of all applications currently supported, by technology domain-ie number and name of each salesforce application, each PowerBuilder application, and each .net application?

ANSWER 11: No

Question 12: What version of PowerBuilder is the SHA currently using/required?

ANSWER 12: Currently PowerBuilder v12.6, migrating to PowerBuilder 2017 at the end of June 2018.

Question 13: What are the COTS products SHA may require assistance in evaluating? Please provide a few examples.

ANSWER13: COTS products are a consideration when new project requests are submitted for review. There are currently no new project requests that require a COTS review at this time.

Question 14: How long has the existing incumbent been in place?

ANSWER 14: Since January 2014.

Question 15: Must each "requirement" in Section 2-3 exactly match the requirements outlined or can we summarize the response?

ANSWER 15: Section 5.4.2 A 2 States: "Proposed Solution: A more detailed description of the Offeror's understanding of the TORFP scope of work, proposed methodology and solution. The proposed solution shall be organized to exactly match the requirements outlined in Sections 2-3." It is up to the Offeror to interpret how they want to address the "proposed services" However, the Proposed Solution under Section 5.4.4.A 2 does request "A more detailed description…" Please review Section 5.4 for detailed instructions for submitting your Technical Proposal.

Question 16: Can MDOT/SHA provide the solicitation in Word?

ANSWER 16: Yes.

Question 17: MBE Subcontracting goal is listed as 20% with the following sub-goals (7% African-American MBEs, 2% Hispanic-American MBEs & 8% for Woman-Owned MBEs). The sub-goals equal 17%; what is the remaining 3% sub goal?

ANSWER 17: Correct, the MBE Subcontracting goal is listed as 20% with the following sub-goals of 7% African-American, 2% Hispanic-American, and 8% Woman-Owned equaling 17%. The remaining 3% MBE is not allocated to a sub-goal, but must be fulfilled by a certified MBE firm.

Question 18: Section 5.4.2, J(b) states "No attachment forms shall be altered." Should we insert the attachment forms as a pdf in the word doc?

ANSWER 18: Form may be submitted in either Word or .PDF format.

Question 19: What is the anticipated start date for J02B8400024?

ANSWER 19: An anticipated start date cannot at this point be determined. However, ideally the Contractor Notice-to-Proceed would be issued a for December start to provide some overlap.

Question 20: Could you please clarify and confirm the overall percentage goal and what would be attributed to the sub-goals when an MBE is the prime?

ANSWER 20: Please see the Answer to Question 6

Question 21: Page 107, 3A is a blank page, is that intentional?

ANSWER 21: Page 107, 3A is not intentional blank. Please see the attached "3A Minimum Qualification Summary" incorporated into revised TORFP document.

Question 22: There is an MBE sub-contracting goal of 20%. We are a MD MDOT certified MBE/DBE firm; what percentage of the overall MBE goal requirement can we take? And do the MBE/Women/Hispanic firms have to be ONLY Maryland certified firms or could they be from other states?

ANSWER 22: Please see the Answer to Question 6. MBE/Women/Hispanic firms do not only have to be from Maryland, but they do have to be certified by MDOT.

Question 23: Who is/are the current incumbent/s providing these services currently and what was the total awarded work order amount per year?

ANSWER 23: Please see the Answer to Question 1. The total awarded Contract amount for the TORFP J02B3400049 can be found on the DOIT web-site: http://doit.maryland.gov/contracts/Pages/CATSPlusTORFPStatus.aspx

Question 24: Are all labor category personnel identified in the TORFP to perform concurrently in a full-time engagement or as needed basis?

ANSWER 24: All personnel brought on-board will be in a full-time engagement.

Question 25: What is the approximate timeframe for SHA to interview the proposed key personnel candidates? Phrased differently, what is the "no-later-than" month that SHA plans to hold interviews for the candidates of short-listed contractors?

ANSWER 25: MDOT/SHA anticipates holding Interviews by October 2018.

Question 26: Can SHA provide a Microsoft Word copy of the TORFP? We will need to fill out the various Attachments that are required to be submitted.

ANSWER 26: See answer to Question 16

Question 27: Can SHA provide a list/inventory of applications that the current resources are responsible for? In addition, can SHA specify the technologies for each of those applications (.NET, SalesForce.com, PowerBuilder, ASP, etc.)? And, can SHA make available to the Offeror for review any documentation for those applications?

ANSWER 27: No.

Question 28: Does SHA have any plans to migrate the existing PowerBuilder application(s) to a .NET environment? If yes, what is the timeframe for migration? And, will any potential migration be part of Scope for this TORFP?

ANSWER 28: No current plans.

Question 29: In the "Key Information Summary Sheet", SHA has specified an overall Minority Business Enterprise (MBE) Goal of 20% with sub-goals of 7% for African American-owned firms; 2% for Hispanic American-owned firms; and 8% for Women-owned firms. As an MBE Prime Contractor, we applaud the State of Maryland, MDOT/SHA and other agencies for their commitment to participation by MBE firms. However, in our opinion, the presence of all the sub-goals in one TORFP itself leads to challenges in the implementation of the project for the contractor. In our opinion, for an efficient execution of the contract, one overall MBE Goal would be preferable over multiple sub-goals. We request MDOT/SHA to either eliminate all the various categories or restrict it to only one category (which can be specified by the State). Will the State consider doing so?

ANSWER 29: No, the State will not change the overall Goal or the Sub-goals.

Question 30: Section 2.1.1 of the TORFP mentions an "incumbent provider". The following are questions pertaining to the "incumbent provider":

a. What is the name of the Contractor company?

b. What are the name(s) of Minority Business Enterprise (MBE) companies that are working under the incumbent provider's contract?

c. What is the Contract Number under which the "incumbent provider" is currently providing services?

d. When (date) is the Contract under which the "incumbent provider" is currently providing services ending?

e. Is the State considering an extension to the Contract under which the "incumbent provider" is currently providing services?

ANSWER 30: a. See Answer to Question 1.
b. Coresphere, LLC; Vikat Solutions LLC; Synergy Systems & Services Inc.
c. J02B3400049
d. December 31, 2018
e. No

Question 31: Section 2.1.1 of the TORFP states that "SHA intends to identify the NTP Date to establish an approximate 10 Business Day transition period with the incumbent provider, SHA intends NTP to be on or around December 10, 2018". Considering the number of resources involved and multiple applications that the resources would be handling, in our opinion, a 10 Business Day transition may not suffice. Will SHA allow or consider a longer transition period – say at least one calendar month?

ANSWER 31: Yes, we would consider extending the 10 Business Day transition. Please note that the Transition would include the 4 Key Personnel and if possible any of the additional personnel that the Contractor is able to provide.

Question 32: Section 2.1.2 of the TORFP states that "SHA intends to award this Task Order to one (1) Master Contractor . . ." Considering the number of resources (eighteen with potential up to twenty resources) involved and the fact that SHA will be managing the selected resources on a day-to-day basis, will SHA consider making awards to multiple contractors? This will allow more than one contractor with qualified resources to be selected.

ANSWER 32: No

Question 33: Section 2.1.3 of the TORFP states that "Master Contractors are advised that, should a solicitation or other competitive award be initiated as a result of activity or recommendations arising from this Task Order, the Offeror awarded this Task Order may not be eligible to compete if such activity constitutes assisting in the drafting of specifications, requirement, or design thereof."

a. Has the current (incumbent) contractor been associated with any one or more of: drafting of specifications, requirement, or design?

b. If yes, would the incumbent contractor be eligible to bid on this TORFP?

ANSWER 33: a. No.
b. If the answer to a. were yes, then the incumbent would not be able to submit a proposal.

Question 34: Section 2.2 "Background and Purpose" of the TORFP mentions (with a bold highlight) that it is MDOT/SHA's "expectation to acquire a TO Contractor who can provide programmers who are multi-skilled in the various programming languages as outlined in sections 1.1 Offeror Personnel Minimum Qualifications and section 2.3 Responsibilities and Tasks". While Section 1.1 specifies the "Offeror Personnel Minimum Qualifications" for the Key Personnel, Section 2.3 is more specific to SHA and contains reference to tools and processes that only the incumbent contractor resources will have experience/expertise in. Can SHA confirm/reassure that the lack of experience/expertise in MDOT/SHA specific tools and expertise is not going to be a disadvantage for contractors other than the incumbent contractor?

ANSWER 34: Lack of knowledge and experience of the general processes and use of the universal tools mentioned in Section 2.3 will be a disadvantage for contractors bidding with unqualified resources.

Question 35: Section 3.10.5 of the TORFP specifies the following positions are considered "Key": Two (2) Senior .Net Programmers; One (1) Senior SalesForce Programmer; and One (1) Senior Power Builder Programmer. Can SHA indicate of the above four (4), which positions will be for the "SHA Headquarters" location and which ones will be for "SHA Hanover Complex" location?

ANSWER 35: Please see the Answer to Question 3

Question 36: We need the following clarification related to Section 3.11 "Substitution of Personnel":

a. Will SHA allow one or more of the four (4) key proposed personnel to be substituted before the oral presentation and/or individual interview?

b. Section 3.11.2 "Substitution of Personnel" for "Prior to and 30 Days After Task Order Execution" talks about substitution being valid under certain circumstances and if the "originally proposed personnel are actual full-time direct employees with the Offeror (subcontractors, temporary staff or 1099 contractors do not qualify)". We believe this requirement is unfair because: (i) some of the proposed personnel (Key or otherwise) will be from our subcontractors / MBE partners and the circumstances described can occur to their personnel as well; and (ii) given the requirements of the TORFP, we may choose to submit personnel who are extremely qualified but are not current employees (rather they would be contingent hires). If the award timeframe is going to take a few months, then these proposed personnel may not be available before the Task Order is executed. Considering the above, we request MDOT/SHA to allow substitution due to non-availability of personnel without a need for them to be "full-time direct employees". Will the State grant this request?

ANSWER 36: a. See Answer to Question 9. b. No

Question 37: Section 4.5 "Oral Presentation" of the TORFP talks about "oral presentation" by the Offeror and/or "interviews" of proposed personnel. Can MDOT/SHA clarify if it intends to have an oral presentation with all the proposed resources present in the oral presentation (i.e., a "group" interview with the Offeror being present) or separate interviews for each of the proposed personnel?

ANSWER 37: MDOT/SHA intends to interview all of the Key Personnel together at one time.

Question 38: Section 5.3.5 A. 3. and Section 5.3.5 B. 3. of the TORFP talks about submitting "a second searchable PDF copy of the Technical Proposal, redacted . . ." and "a second searchable Adobe copy of the TO Financial Proposal, redacted . . ." respectively. Considering the unnecessary burden that this would put on the companies responding to the TORFP (to identify and redact specific areas of the proposal response), can MDOT/SHA remove this requirement of submitting a redacted copy at the time of proposal submission? The rationale for this is that MDOT/SHA can ask for a redacted copy if and when someone actually raises a request under the State Public Information Act – which will allow the Offeror time to produce a redacted copy when necessary.

ANSWER 38: No

Question 39: Attachment B-1 "Financial Proposal Form" has a provision in the last row for providing pricing for "Additional Potential Programmers (2) available via Work Order".

a. We think that providing pricing for the two (2) additional / potential programmers should not be an average of pricing for other programmers, instead the Offeror should have the ability to submit a separate pricing for each of the two (2) additional / potential programmers. Will MDOT/SHA consider this suggestion and modify the Attachment B-1?

b. Also, currently in the Table in Attachment B-1 "Financial Proposal Form", under the "CATS+ Labor Category" column for the "Additional Potential Programmers (2)" there is a "N/A". It is our understanding that as per CATS+ Master Contract, every resource needs to be assigned a Labor Category. As such, can MDOT/SHA modify the Attachment B-1 to allow a Labor Category to be specified for each of the two (2) additional / potential programmers?

ANSWER 39: a. Please see the updated Form B-1 Financial Proposal Form. The additional two resources will be acquired through the Work Order if needed.
b. A Labor Category will be assigned through the Work Order Process.

Question 40: "Page 108 of 122" and "Page 111 of 122" in Appendix 3 – Labor Classification Key Personnel Resume Summary Form of the TORFP seems to be asking for the same information twice. Can MDOT/SHA remove one of the two or consolidate the same?

ANSWER 40: No. Appendix 3 form A Minimum Qualifications Summary is an aid to the agency to make a minimum qualification determination. Information on the Minimum Qualification Summary must correspond with Form B Personnel Resume Summary form for the 4 key personnel.

Question 41: Can MDOT/SHA provide a second date to ask follow-up questions based on answers to the questions submitted until April 17, 2018?

ANSWER 41: All reasonable questions will be answered in a timely manner.

Question 42: Assuming that the answers to the questions (which would have been submitted until April 17, 2018) might be available only a week or so later and to allow sufficient time to review those answers, we request MDOT/SHA for an extension in the proposal due date. Will MDOT/SHA grant this request?

ANSWER 42: Not at this time. But MDOT/SHA may reconsider.

Question 43: Reference: Appendix 3A, page 108 of 122. The RFP states: "TORFP Additional Requirements (Insert, if applicable, the additional requirements from Section 1.1 and 2.10 of the CATS+ RFP)" Please clarify what may be defined as "additional requirements." Would these additional requirements be referring to duties as described in Section 2.10 of the CATS+ RFP? If not, then what would constitute additional requirements?

ANSWER 43: "TORFP Additional Requirements" is referring to Section 3.10.3 Personnel Experience. Appendix 3A has been revised.

Question 44: Reference: Appendix 3A, page 108 of 122. Should the details provided in Appendix 3A related to "TORFP Additional Requirements" mirror those for Generalized Experience and Specialized Experience, providing start and end dates, company/job title, and relevant work experience? If not, how should the details be represented?

ANSWER 44: See answer to Question 43. Yes, the details provided by the Offeror for Appendix 3A "TORFP Additional Requirements" should mirror those for Generalized and Specialized Experience. Provide start and end dates, company/job title, and relevant work experience.

Question 45: Reference: Section 5.4.2, Item J, page 35 of 122. The RFP states: "No attachment forms shall be altered." Please confirm that, though offerors are not to alter the form, offerors are allowed to recreate the form in Word in order to properly complete it. If

not, please provide a Word version in order that offerors may provide the needed information with the appropriate space required.

ANSWER 45: See answer to Question 16. A word version will be released.

Question 46: Reference: Section 3.12.2, page 23 of 122. The subsections for this requirement start with D, and then proceed to only number the subsections that follow with 2 and 3. Is there data missing? Should there be an A, B, and C preceding the D, as well as a 1 preceding the 2 and 3 within D? If not, please provide the correct numbering.

ANSWER 46: The D should be a 1

Question 47: Reference: Attachment B, B-1 Financial Proposal Form, page 46 of 122. The RFP states: "If option years are included, Offerors must submit pricing for each option year." Considering that pricing is to be submitted for each option year, will the state be amending the Financial Proposal Form to allow for a total price per year as opposed to just an hourly rate per year? If the Financial Proposal Form will not be amended, please confirm that the total price for all years is to be included in column G "Extended Price" by multiplying the rate for each year by the total class hours per year in column F, i.e., (AxF) + (BxF) + (CxF) + (DxF) + (ExF).

ANSWER 47: Please see the updated attached Price Proposal Form

Question 48: Will the incumbent be providing the SHA with a Transition-Out Plan similar to the requirement in TORFP Section 3.2.4.A? If so, will this be shared with the new Master Contractor?

ANSWER 48: There was no formal "Transition-Out Plan" requirement stated in the previous TORFP.

End of Addendum #2

CONSULTING AND TECHNICAL SERVICES+ (CATS+)

TASK ORDER REQUEST FOR PROPOSALS (TORFP)

MARYLAND DEPARTMENT OF TRANSPORTATION STATE HIGHWAY ADMINISTRATION (SHA)

SOLICITATION NUMBER J02B8400024

SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP

ISSUE DATE: APRIL 4, 2018

ADDENDUM #2 APRIL 24, 2018

MARYLAND DEPARTMENT OF TRANSPORTATION STATE HIGHWAY ADMINISTRATION (SHA)

KEY INFORMATION SUMMARY SHEET

Solicitation Title:	**SHA APPLICATION PORTFOLIO BUSINESS SERVICES**
Solicitation Number (TORFP#):	**J02B8400024**
Functional Area:	**Functional Area #1 - Enterprise Service Provider (ESP)**
TORFP Issue Date:	Wednesday, April 4, 2018
TORFP Issuing Office:	Maryland Department of Transportation for the State Highway Administration (MDOT/SHA or the "Agency")
Agency Location:	SHA, 707 N. Calvert Street, Baltimore MD 21202
TO Procurement Officer: **e-mail:** **Office Phone:**	Peggy Tischler ptischler@mdot.state.md.us ptischler@mdot.state.md.us 410-865-2777
TO Manager: **e-mail:** **Office Phone:**	Mark W Harrison SHA Headquarters, Office of Information Technology, 707 N. Calvert St., Baltimore, MD 21202 Mharrison3@sha.state.md.us 410-545-8652
TO Proposals are to be sent to:	ptischler@mdot.state.md.us;
TO Pre-proposal Conference:	7201 Corporate Center Drive, Hanover MD 21076, 4th Floor Board Room Wednesday, 4/11/2018 at 10:00 AM – 11:30 AM (EST) See **Attachment 6** for directions.
TO Proposals Due (Closing) Date and Time:	~~Monday, 5/7/2018 at 2:00 PM (EST);~~ **Friday, 5/11/2018 at 2:00 PM (EST)** Offerors are reminded that a completed Feedback Form is requested if a no-bid decision is made (see **Section 5**).
MBE Subcontracting Goal:	20% - with the following sub-goals: 7% for African-American MBEs, 2% for Hispanic-American MBEs, and 8% for Woman-Owned MBEs.
VSBE Subcontracting Goal:	0%

Task Order Type:	Time and Material with Fixed Price and Time and Material Work Orders
Task Order Duration:	Five (5) years, commencing on date of Notice-to-Proceed.
Primary Place of Performance:	Thirteen (13) initial TO Contractor resources located at: SHA Headquarters Office of Information Technology (OIT) 707 N. Calvert St., Baltimore, MD 21202 Five (5) initial TO Contractor resources located at: SHA Hanover Complex Office of Traffic and Safety 7491 Connelly Dr., Hanover, MD 21076
SBR Designation:	No
Federal Funding:	No
Questions Due Date and Time	Tuesday, 4/17/2018 at 2:00 PM (EST)

TABLE OF CONTENTS - TORFP

1 Minimum Qualifications

1.1 Offeror Personnel Minimum Qualifications

Only Offeror Key Personnel that meet the following minimum qualification criteria shall be eligible for consideration in the evaluation of this TORFP. (See Section 3.10.5 – Key Personnel Identified)

The Key personnel proposed under this TORFP and any proposed personnel in response to a Work Order must meet all minimum qualifications for the labor category proposed, as identified in the CATS+ RFP Section 2.10. Resumes shall clearly outline starting dates and ending dates for each applicable experience or skill. Refer to CATS+ RFP Section 2.10 for examples of duties and the required education, general and specialized experience for the Key Personnel.

Offeror must specify the labor category corresponding to the following position(s) listed below and on Attachment B - TO Financial Proposal Form:

1.1.1 Senior **.**Net Programmer

i. Six (6) years of professional experience working in the .Net Framework (all of: C#.net, ASP.net, and VB.net)

ii. Six (6) years of professional experience with all of: JavaScript programming, HTML, XML/XSL, and CSS

1.1.2 Senior SalesForce.com Programmer

i. Six (6) years of professional experience with VisualForce/APEX

ii. One (1) year of professional experience with Lightning Components

1.1.3 Senior PowerBuilder Programmer

i. Six (6) years of professional experience developing applications with PowerBuilder with at least one (1) year experience with PowerBuilder v12.6.

As proof of meeting experience requirements, references must be furnished that are able to attest to the Offeror Personnel Minimum Qualifications as well as meeting the identified labor category description as described in CATS+ RFP Section 2.10 (http://doit.maryland.gov/contracts/Documents/CATSPlus2016/060B2490023-2016CATSPlus2016RFP.pdf

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

2 TO Contractor Requirements: Scope of Work

2.1 Summary Statement

The Maryland Department of Transportation (MDOT) is issuing this CAT+ TORFP for the State Highway Administration (SHA or the "Agency") in order to augment the SHA OIT application support services with a minimum of eighteen (18) highly qualified technical programming resources in accordance with the scope of work described in this TORFP.

2.1.1 In addition to the initial four (4) resources who will be available as of NTP Date, SHA anticipates issuing a Work Order immediately upon Task Order award for fourteen (14) additional resources according to the Work Order Process in **Section 3.14**. SHA will have the option of adding up to two (2) additional resources**, if needed, through the work order process** to this Task Order for a maximum total of twenty (20) resources. All resources beyond the initial eighteen will be requested, as needed through a Work Order process (See **Section 3.14**). SHA intends to identify the NTP Date to establish an approximate 10 Business Day transition period with the incumbent provider, SHA intends NTP to be on or around December 10, 2018.

2.1.2 SHA intends to award this Task Order to one (1) Master Contractor that proposes a team of resources and a Staffing Plan that can best satisfy the Task Order requirements.

2.1.3 Master Contractors are advised that, should a solicitation or other competitive award be initiated as a result of activity or recommendations arising from this Task Order, the Offeror awarded this Task Order may not be eligible to compete if such activity constitutes assisting in the drafting of specifications, requirement, or design thereof.

2.1.4 A Task Order award does not assure a TO Contractor that it will receive all Agency business under the Task Order.

2.2 Background and Purpose

The SHA is responsible for all interstates, U.S. and Maryland numbered routes excluding those in Baltimore City and toll facility-maintained highways. The State system includes approximately 6,000 centerline miles, (16,064 lane miles) of highways and 2,400 bridges, connecting all regions of the State.

The SHA Business overview is available online at: www.roads.maryland.gov.

The SHA Office of Information Technology (OIT) application services section provides application support to its user base as follows:

A. Production issues: this is priority one and addresses any issues with a live production version of an application that hinders or prevents users from performing their duties, or that has a negative impact on the organization.

B. Enhancements to existing production versions: this requires new code to add enhanced features or capabilities to an existing application.

C. New applications: more in-depth functionality, and closely tied to the Advertising Schedule.

There will be occasions where programmers shall share the responsibility in addressing application bugs and new application enhancements as well as the development of other new project assignments based on workload and demand. **It is our expectation to acquire a TO Contractor who can provide programmers who are multi-skilled in the various programming languages as outlined in sections 1.1 Offeror Personnel Minimum Qualifications and section 2.3 Responsibilities and Tasks.**

There are currently two separate development groups, one located in Hanover, MD at: 7491 Connelly Drive, Hanover MD 21076 and the other in downtown Baltimore at: 707 N. Calvert street, Baltimore MD 21202.

2.2.1 Existing Software

A. Maximo is used as the SHA Help Desk tool to record, manage and report on service requests

B. Team Foundation Server is used for configuration and change management

2.2.2 State Staff and Roles

In addition to the TO Manager, the TO Contractor Personnel should expect to interact with other SHA personnel and contractors to meet the Agency's needs. Roles that will be working closely with the TO Contractor Personnel include, but are not limited to:

A. Business Analyst (this is typically a contractor)

The Business Analyst (BA) is responsible for analyzing the business process associated with each project request. The BA will produce detailed requirements that the programmer will use to develop code relevant to the application request.

B. Project Manager (this could be a SHA employee or a contractor)

The Project Manager (PM) is responsible for the facilitation and integration of efforts that are part of the project solution. The PM will work closely with the programmer and the customer. The PM is a certified Project Management Professional (PMP) that utilizes the methodologies as described in the Project Managers Book of Knowledge (PMBOK), part of the Project Management Institute (PMI).

C. Document Specialist (this is typically a contractor)

The Documentation Specialist (DS) is responsible for assisting in the development of the project references in association with the programmer. These references include the technical guide, user guide, and other references as needed.

D. Database Administrator (this is typically a contractor)

The Database Administrator (DBA) is responsible for data centric efforts related to a project. Some of the common efforts that the DBA and programmer will be involved in deal with data integration and properly mapping values to a project's data repository, and reviewing data for security sensitivity, such as Personally Identifiable Information (PII).

E. Web Services (this could be a SHA employee or a contractor)

The Web Services group will work closely with the programmer to deploy web based applications. The collaboration involves identifying the technical information needed to deploy to production, rollback plans, and customer contact information.

F. Network Administrator (this could be a SHA employee or a contractor)

The Network Administrator will be available to work with the programmer in establishing new network connectivity as well as any production issues with current connectivity.

G. Customers (typically a SHA employee)

The programmer will be involved with Joint Application Design (JAD) sessions with the customer and project team. There will be times when the programmer will need to work closely with the customer to gain a deeper understanding of project requirements and customer concerns.

H. Application Support Manager (typically a SHA employee)

The programmer will report to the Application Support Manager (ASM). The ASM will assign work to the programmer, review the programmer's weekly activity, and manager any conflicts the programmer may encounter.

2.2.3 Other State Responsibilities

A. The State will provide normal office working facilities and equipment reasonably necessary for TO Contractor performance under this Task Order. Any special requirements (e.g., reprographic services, computer time, key data entry) shall be identified.

B. The State is responsible for providing required information, data, documentation, and test data to facilitate the TO Contractor's performance of the work, and will provide such additional assistance and services as is specifically set forth.

2.3 Responsibilities and Tasks

2.3.1 General Responsibilities

A. TO Contractor Personnel shall provide technical expertise and advice to SHA staff and management.

B. TO Contractor Personnel shall assist the PM and BA in the preparation of documentation to describe new or changed processes.

C. TO Contractor Personnel shall respond to information requests that business users submit through SHA's Maximo Automated Help Desk Application (Maximo) or the Office of Traffic and Safety (OOTS) IT Help Desk.

D. TO Contractor Personnel shall respond to trouble reports or change requests (TR / CR Log) reported through Maximo or the OOTS IT Help Desk.

E. TO Contractor Personnel shall assist in research and recommendations on new technologies.

F. TO Contractor Personnel shall assist in the development of Microsoft Software Storage Client (MSSC) objects used to implement and upgrade client software.

G. TO Contractor Personnel shall assist in the preparation and implementation of disaster recovery plans for various systems. TO Contractor Personnel shall create upgrade and migration schedules with plans that will minimize the impact on production and mission critical systems.

H. TO Contractor Personnel shall train end users on assigned applications, as needed.

I. TO Contractor Personnel shall attend organizational meetings as directed.

2.3.2 Existing System Maintenance Responsibilities

A. TO Contractor Personnel shall provide ongoing support for various SHA applications and technologies, as assigned.

B. TO Contractor Personnel shall maintain a TR and CR Log for each assigned application using Team Foundation Server or SharePoint environments, as directed.

C. TO Contractor Personnel shall remediate application defects reported through Maximo, OOTS IT Help Desk or from the business side System Administrators.

D. TO Contractor Personnel shall evaluate, design, and code approved application CRs.

E. TO Contractor Personnel shall perform integration testing any code and configuration changes prior to releasing for User Acceptance Testing (UAT).

F. TO Contractor Personnel shall maintain configuration and version control using Team Foundation Server.

G. TO Contractor Personnel shall assist in the development of application maintenance plans for scheduled maintenance activities.

H. TO Contractor Personnel shall recommend and assist in the development and implementation of maintenance plans for system upgrades and technology refreshes.

I. TO Contractor Personnel shall, in conjunction with the PM and BA, maintain and update System Documentation including but not limited to:

1. Interface Control Documents
2. User Guides
3. Administrator Guides
4. Test Cases
5. Release Notes
6. Security Procedures

J. TO Contractor Personnel shall develop system source code and executables using, but not limited to, the following primary technologies:

1. Microsoft Access 2007 or later version
2. C#.NET,
3. VB.NET,
4. SalesForce.com VisualForce/APEX, Lightning components
5. PowerBuilder v12.6,
6. Visual Basic 6.0,
7. ASP.NET
8. ASP 3.0
9. Delphi

2.3.3 New System Development Responsibilities

A. TO Contractor Personnel shall assist the PM in the gathering and development of system requirements.

B. TO Contractor Personnel shall analyze, recommend and design appropriate system security according to policies for data and application security using MDOT and DoIT's security standards.

C. TO Contractor Personnel shall recommend system design and participate in design revision reviews.

D. TO Contractor Personnel shall design the data model used by the application.

E. TO Contractor Personnel shall develop system source code and executables using, but not limited to, one of the following primary technologies:

1. Microsoft Access 2007 or later version
2. C#.NET,
3. ASP.NET,
4. VB.NET,
5. SalesForce.com VisualForce/APEX
6. SalesForce1 and Lightning components
7. PowerBuilder v12.6 or later version

F. TO Contractor Personnel shall maintain Configuration and Version Control using Team Foundation Server.

G. TO Contractor Personnel shall, in conjunction with the PM and BA, prepare repeatable test plans for rigorous testing of database servers and application upgrades.

H. TO Contractor Personnel shall perform unit, integration, and system testing.

I. TO Contractor Personnel shall maintain Test Problem Report through the use of Team Foundation Server or SharePoint environments.

J. TO Contractor Personnel shall assist with the installation and implementation of Agency-approved new application system software.

K. TO Contractor Personnel shall, in conjunction with the PM and BA, assist with the development of System Documentation including but not limited to:

1. Design Document
2. Interface Control Documents
3. Source Code Documents
4. Test Data and Test Cases
5. Test Reports with Results
6. Users Guides
7. Administrator Guides
8. Implementation Plan
9. Release Notes
10. Security Procedures

L. TO Contractor Personnel shall maintain a TR / CR Log for new application through the use of Team Foundation Server or SharePoint environments.

2.3.4 Non-Functional, Non-Technical Requirements

A. TO Contractor Personnel shall be responsible for knowledge transfer, occurring on the reassignment of a project resource from one task/project to another (either permanent or temporary transfer).

B. TO Contractor Personnel shall complete SHA-mandated core training prior to arrival to assigned SHA facilities

1. Each TO Contractor resource assigned to work on-site at an SHA facility and or SHA project site for a period of three (3) months or longer, regardless of the number of days worked per week, shall be required to take the following four (4) MANDATORY TRAINING COURSES given to all SHA employees and on-site TO Contractors:

a) ADA Awareness

b) Limited English Proficiency

c) Sexual Harassment Awareness

d) Workplace and Domestic Violence Awareness

2. This MANDATORY TRAINING shall be completed prior to the on-site TO Contractor resource's start date at the SHA facility (and/or project site). **Failure to complete this training prior to the resources start date could be grounds for termination.**

3. Each on-site TO Contractor resource shall provide certification of training completion by printing the certificate of completion available at the end of each training course and furnishing the printed copy to the TO Manager as record of completion

4. The on-site TO Contractor resource shall also forward a copy of all training certificates to the TO Contractor for its contract management records.

5. The TO Contractor cannot bill the hours required for its resources to complete this MANDATORY TRAINING. The hours estimated to complete all four (4) training courses is approximately 8 hours and will be available on-line from SHA's Internet Web site. There will be no cost for materials or the training course itself.

C. TO Contractor Personnel shall participate in meetings as a technical resource, as required.

D. TO Contractor Personnel shall support annual SHA initiatives involving technology of applications, such as the annual SHA online employee survey.

E. TO Contractor Personnel shall be responsible for reviewing technical documentation that may be authored by other resources for correctness.

F. TO Contractor Personnel shall, in conjunction with the PM, conduct training for end users, as necessary.

G. TO Contractor Personnel shall maintain workstations, including cleaning and reinstalling after a re-image.

H. TO Contractor Personnel shall perform product assessment of new technology as directed by the Agency.

I. TO Contractor Personnel shall attend technology or skill training, as required, at no cost to the Agency, to include, but not be limited to training that ensures TO Contractor Personnel (see Section 3.10.11):

1. To be competent in the practical use of new versions of existing SHA technologies,

2. To be competent in the practical use of new SHA technologies, and

3. To elevate competency with existing SHA technologies.

J. TO Contractor Personnel shall enter information into OIT's portfolio management software (Innotas) including status updates and time spent on projects.

2.3.5 Required Project Policies, Guidelines and Methodologies

The TO Contractor shall be required to comply with all applicable laws, regulations, policies, standards and guidelines affecting Information Technology projects, which may be created or changed periodically. Offeror is required to review all applicable links provided below and state compliance in its response.

It is the responsibility of the TO Contractor to ensure adherence and to remain abreast of new or revised laws, regulations, policies, standards and guidelines affecting project execution. These include, but are not limited to:

A. The State of Maryland System Development Life Cycle (SDLC) methodology at: www.DoIT.maryland.gov - keyword: SDLC;

B. The State of Maryland Information Technology Security Policy and Standards at: www.DoIT.maryland.gov - keyword: Security Policy;

C. The State of Maryland Information Technology Non-Visual Standards at: http://doit.maryland.gov/policies/Pages/ContractPolicies.aspx;

D. The State of Maryland Information Technology Project Oversight at: http://doit.maryland.gov/epmo/Pages/MITDP/oversight.aspx;

E. The TO Contractor shall follow project management methodologies consistent with the most recent edition of the Project Management Institute's *Project Management Body of Knowledge Guide*; and

F. TO Contractor Personnel shall follow a consistent methodology for all Task Order activities.

G. MDOT Information Security Plan (See Appendix 5)

H. MDOT ITIL Procedures and Practices as approved and implemented by MDOT.

2.3.6 Staffing Plan

Offerors shall describe in a Staffing Plan how all of the following additional resources, those other than the four (4) Key resources, shall be acquired to meet the needs of the Agency. Each job role below may be paired with a single CATS+ labor category. See Section 2.10 of the CATS+ Master Contract.

A. Eight (8) additional .Net Programmers
Each .Net Programmer is expected to possess the following experience:
   i. Four (4) years of professional experience working in the .Net Framework (C#.net, ASP.net or VB.net)
   ii. Four (4) years of professional experience with JavaScript programming, HTML, XML/XSL, and CSS

B. Two (2) additional Senior .Net Programmers
Each Senior .Net Programmer is expected to possess the following experience:
   i. Six (6) years of professional experience working in the .Net Framework (C#.net, ASP.net or VB.net)
   ii. Six (6) years of professional working experience with JavaScript programming, HTML, XML/XSL, and CSS

C. Two (2) additional SalesForce.com Programmers
Each SalesForce.com Programmer is expected to possess the following experience:
i. Four (4) years of professional experience with VisualForce/APEX
ii. One (1) year of professional experience with Lightning Components

D. One (1) additional Senior SalesForce.com Programmer
Each Senior SalesForce.com Programmer is expected to possess the following experience:
i. Six (6) years of professional working experience with VisualForce/APEX
ii. One (1) year of professional working experience with Lightning Components

E. One (1) additional PowerBuilder Programmer
Each PowerBuilder Programmer is expected to possess the following experience:
i. Four (4) years of professional experience developing applications with PowerBuilder with at least one (1) year experience with PowerBuilder v12.6

2.4 Deliverables

2.4.1 Deliverable Descriptions/Acceptance Criteria

A. TO Contractor Personnel shall produce, contribute to, and revise work products and deliverables as directed by the Agency.

B. TO Contractor Personnel shall recommend work products and deliverables for best execution of the Agency's needs.

ID #	Deliverable Description	Acceptance Criteria	Due Date / Frequency
1	Weekly TO Contractor Personnel Status Reports	Microsoft Word template (see Appendix 6) that contains the following: a. Activities completed with hours of effort, b. Activities in progress with hours of effort, c. Next weeks planned activities, d. Activities on hold/issues, e. Activities requiring overtime with hours of effort, f. Action items	Weekly TO Contractor Personnel Status Report emailed to the Application Services Manager by Friday Close of Business (COB)
2	Minority Business Enterprise (MBE) Report	See Section 3.12	See Section 3.12
3	TORFP progress, budget and MBE review session	A meeting with the TO Manager and OIT leadership to review progress on the TORFP including budget and the MBE goal.	Yearly to fall within 2 weeks of the anniversary of the NTP.

2.5 Optional Features, Future Work

2.5.1 Change Orders

A. If the TO Contractor is required to perform work beyond the scope of this TORFP, or there is a work reduction due to unforeseen scope changes, a TO Change Order is required. The TO Contractor and TO Manager shall negotiate a mutually acceptable price modification based on the TO Contractor's proposed rates in the Master Contract and scope of the work change.

B. No scope of work changes shall be performed until a change order is approved by DoIT and executed by the TO Procurement Officer.

2.6 Service Level Agreement (SLA)

THIS SECTION IS NOT APPLICABLE TO THIS TORFP.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

3 TO Contractor Requirements: General

3.1 Task Order Initiation Requirements

A. TO Contractor shall schedule and hold a kickoff meeting within 10 Business Days after NTP Date. At the kickoff, the TO Contractor shall furnish/review:

1. The Staffing Plan execution
   i. Time table for resume review
   ii. Time table for interviews
   iii. Time table for on-boarding
2. The plan for transition
   i. Application knowledge transfer
   ii. Toolset knowledge transfer
   iii. Standard Operating Procedures
   iv. Best practices utilized
3. Any questions that need clarification

B. Individual TO Contractor Personnel shall complete the mandatory training prior to presenting themselves for Agency on-site work. See **2.3.4.B.**

3.2 End of Task Order Transition

3.2.1 The TO Contractor shall provide transition assistance as requested by the State to facilitate the orderly transfer of services to the State or a follow-on contractor, for a period up to 30 working days prior to Task Order end date, or the termination thereof. Such transition efforts shall consist, not by way of limitation, of:

A. Provide additional services and/or support as requested to successfully complete the transition;

B. Maintain the services called for by the Task Order at the required level of proficiency;

C. Provide updated System Documentation, as appropriate; and

D. Provide current operating procedures (as appropriate).

3.2.2 The TO Contractor shall work toward a prompt and timely transition, proceeding in accordance with the directions of the TO Manager. The TO Manager may provide the TO Contractor with additional instructions to meet specific transition requirements prior to the end of Task Order.

3.2.3 The TO Contractor shall ensure that all necessary knowledge and materials for the tasks completed are transferred to the custody of State personnel or a third party, as directed by the TO Manager.

3.2.4 The TO Contractor shall support end-of-Task Order transition efforts with technical and project support to include but not be limited to:

A. The TO Contractor shall provide a draft Transition-Out Plan 120 Business Days in advance of Task Order end date.

B. The Transition-Out Plan shall address at a minimum the following areas:

1. Any staffing concerns/issues related to the closeout of the Task Order;
2. Communications and reporting process between the TO Contractor, the Agency and the TO Manager;
3. Security and system access review and closeout;
4. Any hardware/software inventory or licensing including transfer of any point of contact for required software licenses to the Agency or a designee;
5. Any final training/orientation of Agency staff;
6. Connectivity services provided, activities and approximate timelines required for Transition-Out;
7. Knowledge transfer, to include:
   a) A working knowledge of the current system environments as well as the general business practices of the Agency;
   b) Review with the Agency the procedures and practices that support the business process and current system environments;
   c) Working knowledge of all technical and functional matters associated with the Solution, its architecture, data file structure, interfaces, any batch programs, and any hardware or software tools utilized in the performance of this Task Order;
   d) Documentation that lists and describes all hardware and software tools utilized in the performance of this Task Order;
   e) A working knowledge of various utilities and corollary software products used in support and operation of the Solution;
8. Plans to complete tasks and any unfinished work items (including open change requests, and known bug/issues); and
9. Any risk factors with the timing and the Transition-Out schedule and transition process. The TO Contractor shall document any risk factors and suggested solutions.

C. The TO Contractor shall ensure all documentation and data including, but not limited to, System Documentation and current operating procedures, is current and complete with a hard and soft copy in a format prescribed by the TO Manager.

D. The TO Contractor shall provide copies of any current daily and weekly back-ups to the Agency or a third party as directed by the TO Manager as of the final date of transition, but no later than the final date of the Task Order.

E. Access to any data or configurations of the furnished product and/or services shall be available after the expiration of the Task **Order.**

3.2.5 Return and Maintenance of State Data

This section does not apply

3.3 Invoicing

3.3.1 Definitions

A. "Proper Invoice" means a bill, written document, or electronic transmission, readable by the agency, provided by a vendor requesting an amount that is due and payable by law under a written

procurement contract for property received or services rendered that meets the requirements of COMAR 21.06.09.02.

B. "Late Payment" means any amount that is due and payable by law under a written procurement contract, without deferral, delay, or set-off under COMAR 21.02.07.03, and remains unpaid more than 45 days after an agency receives a Proper Invoice.

C. "Payment" includes all required processing and authorization by the Comptroller of the Treasury, as provided under COMAR 21.02.07, and may be deferred, delayed, or set-off as applicable under COMAR 21.02.07.03.

3.3.2 General

A. Invoice payments to the TO Contractor shall be governed by the terms and conditions defined in the CATS+ Master Contract.

B. Any on-call hours and upgrades performed during non-Business Hours shall be billed based on actual time worked at the approved Task Order labor rates.

C. The TO Contractor shall send the original of each invoice and supporting documentation (itemized billing reference for employees, including detail of work) to:

1) E-Mail: sha-oit-invoice@sha.state.md.us for OIT assigned resources

2) E-Mail: Office of Traffic and Safety, point of contact will be named after award

3) The TO Manager's name must be shown on the E-mail Subject Line

D. Invoices for final payment shall be clearly marked as "FINAL" and submitted when all work requirements have been completed and no further charges are to be incurred under the TO Agreement. In no event shall any invoice be submitted later than 60 calendar days from the TO Agreement termination date.

E. Invoices submitted without the required information cannot be processed for payment. Payment of invoices may be withheld if any required documentation is not submitted including without limitation status reports. A Proper Invoice, required as Payment documentation, must include the following information, without error:

1. TO Contractor name and address;
2. TO Contractor point-of-contact with telephone number;
3. Remittance address;
4. Federal taxpayer identification (FEIN) number, social security number, as appropriate;
5. Invoice period (i.e. time period during which services covered by invoice were performed);
6. Invoice date;
7. Invoice number;
8. State assigned TO Agreement number and Title;
9. SHA issued (Blanket) Purchase Order number(s);
10. Labor Category;
11. Services provided broken down by specific resource to include Labor Category and quantity.

12. Amount due; and
13. Award amount;
14. Amount billed to date;
15. Amount remaining on contract;
16. MBE award amount;
17. MBE amount billed to date;
18. MBE percentage committed;
19. Any additional documentation required by regulation or the Task Order.

3.3.3 Invoice Submission Schedule

The TO Contractor shall submit monthly invoices for SHA approval and payment that coincide with the submission of the Weekly TO Contractor Personnel Status Reports for the month on or before the 10th day of the month. The invoices shall identify actual hours by each person assigned to the Task Order during the reporting period. Invoices shall be accompanied by timesheets documenting charges for labor in accordance with the TO Financial Proposal.

Invoices and all required documentation shall reflect the first day of the month through the last day of the month, **only**. Any piece of documentation showing hours worked the days before or after any given documented month will be incorrect and the TO Contractor shall be required to resubmit the entire package. Any documentation received after the 10th day of any month will be considered late. If the 10th of any month falls on a weekend, government holiday, or State of Maryland Service Reduction day, all documentation is due the last government Business Day prior.

It shall be the sole responsibility of the TO Contractor to ensure that all required monthly documentation is received by the 10th of each month.

3.3.4 For the purposes of this Task Order an amount will not be deemed due and payable if:

A. The amount invoiced is inconsistent with the Task Order.

B. The proper invoice has not been received by the party or office specified in the Task Order.

C. The invoice or performance is in dispute or the TO Contractor has failed to otherwise comply with the provisions of the Task Order.

D. The item or services have not been accepted.

E. The quantity of items delivered is less than the quantity ordered.

F. The items or services do not meet the quality requirements of the Task Order

G. If the Task Order provides for progress payments, the proper invoice for the progress payment has not been submitted pursuant to the schedule.

H. The TO Contractor has not submitted satisfactory documentation or other evidence reasonably required by the TO Procurement Officer or by the contract concerning performance under the contract and compliance with its provisions.

3.3.5 Travel Reimbursement

A. There shall be no reimbursement for Routine Travel. TO Contractor shall not be reimbursed for Non-Routine Travel without prior TO Manager approval.

B. Routine Travel is defined as travel within a 50-mile radius of the Agency's base location, as identified in the TORFP, or the TO Contractor's facility, whichever is closer to the consulting site. There will be no payment for labor hours for travel time or reimbursement for any travel expenses for work performed within these radiuses or at the TO Contractor's facility.

C. Non-routine Travel is defined as travel beyond the 50-mile radius of Agency's base location, as identified in the TORFP, or the TO Contractor's facility, whichever is closer to the consulting site. Non-routine travel will be identified within a TO Agreement, if appropriate, and will be reimbursed according to the State's travel regulations and reimbursement rates, which can be found at: www.DBM.maryland.gov - search: Fleet Management. If non-routine travel is conducted by automobile, the first 50 miles of such travel will be treated as routine travel and as described in **Section 3.3.7.A**, and will not be reimbursed. The TO Contractor may bill for labor hours expended in non-routine traveling beyond the identified 50-mile radius, only if so specified in the TORFP or Work Order.

3.3.6 Retainage

This section does not apply to this TORFP.

3.4 Liquidated Damages

MBE Liquidated damages are identified in **Attachment M**.

This solicitation does not require additional liquidated damages.

3.5 Disaster Recovery and Data

The following requirements apply to the TO Agreement:

3.5.1 Redundancy, Data Backup and Disaster Recovery

A. Resources shall be required to support SHA disaster recovery according to SHA's Disaster Recovery Plan and as assigned by SHA.

B. The SHA outlines its complete application restoration strategy for each application in its Disaster Recovery Plan. The developer portion of the disaster recovery plan for each application can be roughly summarized as follows (with the assumption that any hardware asset recovery has already been completed by OIT's Network & Desktop support group):

1. Attempt to restore the application installation directly from the Business Day Backup archive
2. If Step 1 is not feasible, retrieve the source code from Team Foundation Server and reinstall/configure the application manually.
3. In either case, once the application has been re-implemented / restored, the programmer reconnects the application to its data center, either its normal data center, or one restored from Business Day Backups by the Database Administration section.
4. Any additional modules or connections required for normal operation are re-implemented / restored.
5. The programmer tests the application for correctness and declares it ready for operational use if no further corrective action is required.

3.5.2 Data Ownership and Access

A. Data, databases and derived data products created, collected, manipulated, or directly purchased as part of a TORFP shall become the property of the State. The purchasing State agency is considered the custodian of the data and shall determine the use, access, distribution and other conditions based on appropriate State statutes and regulations.

B. Public jurisdiction user accounts and public jurisdiction data shall not be accessed, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of the Task Order, including as necessary to perform the services hereunder or (4) at the State's written request.

C. The TO Contractor shall limit access to and possession of State data to only TO Contractor Personnel whose responsibilities reasonably require such access or possession and shall train such TO Contractor Personnel on the confidentiality obligations set forth herein.

D. At no time shall any data or processes – that either belong to or are intended for the use of the State or its officers, agents or employees – be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

E. The Contractor shall not use any information collected in connection with the services furnished under this Contract for any purpose other than fulfilling such services.

3.5.3 Provisions in Sections 3.5.1 – 3.5.2 shall survive expiration or termination of the TO Agreement. Additionally, the TO Contractor and shall flow down the provisions of Sections 3.5.1-3.5.2 (or the substance thereof) in all subcontracts.

3.6 Insurance Requirements

3.6.1 Offeror shall confirm that, as of the date of its proposal, the insurance policies incorporated into its Master Contract are still current and effective at the required levels (See Master Contract Section 2.7).

3.6.2 The Offeror shall also confirm that any insurance policies intended to satisfy the requirements of this TORFP are issued by a company that is licensed to do business in the State of Maryland.

3.7 Security Requirements

3.7.1 Employee Identification

A. TO Contractor Personnel shall display his or her company ID badge in a visible location at all times while on State premises. Upon request of authorized State personnel, each such TO Contractor Personnel shall provide additional photo identification.

B. TO Contractor Personnel shall cooperate with State site requirements, including but not limited to, being prepared to be escorted at all times, and providing information for State badge issuance.

C. TO Contractor shall remove any TO Contractor Personnel from working on the Task Order where the State determines, in its sole discretion, that said TO Contractor Personnel has not adhered to the Security requirements specified herein.

D. The State reserves the right to request that the TO Contractor submit proof of employment authorization of non-United States Citizens, prior to commencement of work under the Task Order.

E. Unless otherwise specified, the cost of complying with all security requirements specified herein are the sole responsibility and obligation of the TO Contractor and its subcontractors and no such costs shall be passed through to or reimbursed by the State or any of its agencies or units.

3.7.2 Security Clearance / Criminal Background Checks

A. The TO Contractor shall obtain from all Contractor Personnel assigned to work on the Task Order a signed statement permitting a criminal background check within thirty (30) days after NTP, the TO Contractor shall secure at its own expense the following type of national criminal history record check and provide the TO Contract Manager with completed checks on such Contractor Personnel prior to assignment.

B. A national criminal history record check. This check may be performed by a public or private entity. The State reserves the right to require, when allowed, a fingerprint-based Maryland and/or FBI Criminal Justice Information System criminal history record check.

C. At a minimum, these background checks must include all convictions and probation before judgment (PBJ) dispositions. The TO Contractor may not assign an individual whose background check reflects any criminal activity to work under this Task Order unless prior written approval is obtained from the TO Contract Manager.

D. TO Contractor shall be responsible for ensuring that TO Contractor Personnel background check certifications are renewed annually, and at the sole expense to the TO Contractor.

E. Further, TO Contractor Personnel may be subject to random security checks during entry and exit of State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while on secured premises.

F. TO Contractor shall complete a criminal background check prior to any individual TO Contractor Personnel being assigned work on the project. TO Contractor shall provide a Criminal Background Check Affidavit (Appendix 3) within 30 days of notice to proceed. On-Site Security Requirement(s)

G. For the conditions noted below, TO Contractor Personnel may be barred from entrance or leaving any site until such time that the State's conditions and queries are satisfied.

   1. TO Contractor Personnel may be subject to random security checks when entering and leaving State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while in secured premises.

   2. Some State sites, especially those premises of the Department of Public Safety and Correctional Services, require each person entering the premises to document and inventory items (such as tools and equipment) being brought onto the site, and to submit to a physical search of his or her person. Therefore, TO Contractor Personnel shall always have available an inventory list of tools being brought onto a site and be prepared to present the inventory list to the State staff or an officer upon arrival for review, as well as present the tools or equipment for inspection. Before leaving the site, the TO Contractor Personnel will again present the inventory list and the tools or equipment for inspection. Upon both entering the site and leaving the site, State staff or a correctional or police officer may search TO Contractor Personnel. Depending upon facility rules, specific tools or personal items may be prohibited from being brought into the facility.

H. Any TO Contractor Personnel who enters the premises of a facility under the jurisdiction of the Agency may be searched, fingerprinted (for the purpose of a criminal history background check), photographed and required to wear an identification card issued by the Agency.

I. Further, TO Contractor Personnel shall not violate Md. Code Ann., Criminal Law Art. Section 9-410 through 9-417 and such other security policies of the agency that controls the facility to which the TO Contractor Personnel seeks access. The failure of any of the TO Contractor Personnel to comply with any provision of the TO Agreement is sufficient grounds for the State to immediately terminate the TO Agreement for default.

3.7.3 Information Technology

The TO Contractor shall:

A. Implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry best practices for information security such as those listed below (see **Section 3.7.4**);

B. Ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of the TO Agreement; and

C. The TO Contractor, and TO Contractor Personnel, shall (i) abide by all applicable federal, State and local laws, rules and regulations concerning security of Information Systems and Information Technology and (ii) comply with and adhere to the State IT Security Policy and Standards as each may be amended or revised from time to time. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy, and (iii) the MDOT Information Security Plan in **Appendix 5**.

3.7.4 Data Protection and Controls

TO Contractor shall ensure a secure environment for all State data and any hardware and software (including but not limited to servers, network and data components) to be provided or used in connection with the performance of the TO Agreement and shall apply or cause application of appropriate controls so as to maintain such a secure environment ("Security Best Practices"). Such Security Best Practices shall comply with an accepted industry standard, such as the NIST cybersecurity framework.

A. To ensure appropriate data protection safeguards are in place, the TO Contractor shall implement and maintain the following controls at all times throughout the term of the TO Agreement (the TO Contractor may augment this list with additional controls):

   1. By default, "deny all" and only allow access by exception.

   2. Ensure TO Contractor's Personnel shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The TO Contractor/subcontractor shall complete any necessary paperwork as directed and coordinated with the TO Agreement Monitor to obtain approval by the State to connect TO Contractor/subcontractor-owned equipment to a State LAN/WAN.

3.7.5 Additional security requirements may be established in a Work Order.

3.7.6 The State shall, at its discretion, have the right to review and assess the Contractor's compliance to the security requirements and standards defined in the TO Agreement.

3.7.7 Provisions in Sections 3.7.1 – 3.7.5 shall survive expiration or termination of the TO Agreement. Additionally, the TO Contractor and shall flow down the provisions of Sections 3.7.4-3.7.6 (or the substance thereof) in all subcontracts.

3.8 RESERVED

3.9 SOC 2 Type 2 Audit Report

A SOC 2 Type 2 Report is not a TO Contractor requirement for this Task Order.

3.10 Performance and Personnel

3.10.1 ROLES AND RESPONSIBILITIES

Personnel roles and responsibilities under the Task Order:

A. **TO Procurement Officer** – The TO Procurement Officer has the primary responsibility for the management of the TORFP process, for the resolution of TO Agreement scope issues, and for authorizing any changes to the TO Agreement.

B. **TO Manager** - The TO Manager has the primary responsibility for the management of the work performed under the TO Agreement, administrative functions, including issuing written directions, and for ensuring compliance with the terms and conditions of the CATS+ Master Contract.

   The TO Manager will assign tasks to the personnel provided under this TORFP and will track and monitor the work being performed through the monthly accounting of hours' deliverable for work types; actual work produced will be reconciled with the hours reported.

C. **TO Contractor** – The TO Contractor is the CATS+ Master Contractor awarded this Task Order. The TO Contractor shall provide human resources as necessary to perform the services described in this TORFP Scope of Work.

D. **TO Contractor Manager** – The TO Contractor Manager will serve as primary point of contact with the TO Manager to regularly discuss progress of tasks, upcoming tasking, historical performance, and resolution of any issues that may arise pertaining to the TO Contractor Personnel. The TO Contractor Manager will serve as liaison between the TO Manager and the senior TO Contractor management.

E. **TO Contractor Personnel** – Any official, employee, agent, Subcontractor, or Subcontractor agents of the TO Contractor who is involved with the Task Order over the course of the Task Order period of performance.

F. **Key Personnel** – A subset of TO Contractor Personnel whose departure during the performance period, will, in the State's opinion, have a substantial negative impact on Task Order performance. Key Personnel proposed as part of the TO Proposal shall start as of TO Agreement issuance unless specified otherwise in this TORFP or the Offeror's TO Technical Proposal. Key Personnel may be identified after Task Order award

G. **MDOT Contract Management Office (CMO)** - The CMO is responsible for contract management issues outside of the day to day management of the TO contract after award.

3.10.2 Offeror Experience

The following Offeror experience is expected and will be evaluated as part of the TO Technical Proposal (see the Offeror experience, capability and references evaluation factor from **Section 6.2**):

A. The extent to which the Offeror demonstrates prior experience providing technical business support services, where more desirable experience includes:

   i. Furnishing services to U.S. based commercial or government entities with at least 1,000 end-users.

   ii. Participating in engagements lasting three (3) or more years

   iii. The extent to which the Customer(s) were satisfied with Offeror's performance

   iv. the number of full-time personnel furnished under the engagement, (where 10 or more is considered ideal experience)

B. The extent to which the Offeror has provided multiple full-time resources possessing a current development platform certification (e.g.: a SalesForce or .Net or PowerBuilder developer certification).

C. Offeror's experience with technical business support projects and services similar to those described in the TORFP, as attested by references furnished in the TO Technical Proposal.

3.10.3 Personnel Experience

The following experience is expected and will be evaluated as part of the TO Technical Proposal and references provided (see the capability of proposed resources evaluation factor from **Section 6.2**):

A. The extent to which the programmers have senior level experience in the respective position.

B. For the Senior .Net programmer role, the extent to which the programmer has C#.Net, ASP.Net and VB.Net experience.

3.10.4 Number of Personnel to Propose

As part of the TO Proposal evaluation, Offerors shall propose exactly four (4) personnel who are expected to be available as of the start date specified in the Notice to Proceed (NTP Date). Offerors shall describe in a Staffing Plan how all of the additional resources shall be acquired to meet the needs of the Agency (see Section 2.3.6).

Offerors may generally describe planned positions in a Staffing Plan. Such planned positions may not be used as evidence of fulfilling personnel minimum qualifications.

3.10.5 Key Personnel Identified

For the Task Order, the following positions will be considered Key Personnel, and shall be required to meet the qualifications stated in Section 1.1 and minimum qualification as referenced in Section 2.10 of the CATS+ Master Contract for selected labor categories.

1. Two (2) Senior .Net Programmer2.1
2. One (1) Senior SalesForce Programmer
3. One (1) Senior Power Builder Programmer

3.10.6 Labor Categories

To be responsive to this TORFP, Offerors must be capable of providing and meeting the minimum qualifications for all the labor categories listed. Offerors shall submit a TO Financial Proposal Form (Attachment B) that provides labor rates for all labor categories for all Task Order years (initial term and any option periods). Actual resumes shall be provided only for Key Personnel as described in **Section 3.10.5**. Resumes for resources provided later shall be coordinated by the TO Manager per the TO Technical Proposal and, if requested in a Work Order, shall be governed by the Work Order process.

A. Each Labor Category includes Titles, Position Description, Education and Experience (General and Specialized).

B. Education and experience described below constitute the minimum qualifications for candidates proposed in response to a TORFP. All experience required must have occurred within the most recent ten (10) years.

C. TO Contractor Personnel Experience (including Key Personnel submitted in response to this TORFP).

3.10.7 Substitution of Education for Experience

A Bachelor's Degree or higher may be substituted for the general and specialized experience for those labor categories requiring a High School Diploma. A Master's Degree may be substituted for two years of the general and specialized experience for those labor categories requiring a Bachelor's Degree. Substitution shall be reviewed and approved by the State at its discretion.

3.10.8 Substitution of Experience for Education

A. Substitution of experience for education may be permitted at the discretion of the State.

B. Substitution of Professional Certificates for Experience:

C. Professional certification (e.g., Microsoft Certified Solutions Expert, SQL Certified Database Administrator) may be substituted for up to two (2) years for general and specialized experience at the discretion of the State.

3.10.9 TO Contractor Personnel Maintain Certifications

Any TO Contractor Personnel provided under this TORFP shall maintain in good standing any required professional certifications for the duration of the TO Agreement.

3.10.10 Work Hours

A. Hours of Operation Support: The TO Contractor shall assign TO Contractor Personnel to support the Agency hours of operation; 08:00 AM to 04:30 PM, Monday through Friday except for MDOT holidays.

B. Needs beyond the hours described in paragraph A may be defined in a Work Order.

C. TO Contractor Personnel may also be required to provide occasional support outside of normal Agency hours of operation, including evenings, overnight, and weekends, to support specific efforts and emergencies, such as to resolve system repair or restoration. Hours performing activities would be billed on an actual time worked basis at the rates proposed.

D. Any work beyond given parameters requires prior approval from the TO Manager is included; an example is: "Unless otherwise directed by the TO Manager, the TO Contractor's assigned personnel will work an eight-hour day (Hours to be approved by TO Manager,) Monday through Friday except for SHA Holidays (including but not limited to Service Reduction Days or Mandatory State Furlough Days)."

E. State-Mandated Closings: TO Contractor Personnel shall be required to participate in any State-mandated closings. In this event, the TO Contractor will be notified in writing by the TO Manager of these details.

F. Minimum and Maximum Hours: Full-time TO Contractor Personnel shall work 40 hours per week with starting and ending times as approved by the TO Manager. A flexible work schedule may be used with TO Manager approval, including time to support any efforts outside core business hours. TO Contractor Personnel may also be requested to restrict the number of hours TO Contractor personnel can work within a given period of time that may result in less than an eight-hour day or less than a 40-hour work week.

G. Vacation Hours: Requests for leave shall be submitted to the TO Manager at least two weeks in advance. The TO Manager reserves the right to request a temporary replacement if leave extends

longer than one consecutive week. In cases where there is insufficient coverage, a leave request may be denied.

3.10.11 Professional Development

Technology and software products continuously change. The TO Contractor shall ensure continuing education opportunities for the personnel provided. This education shall be associated with the technologies currently utilized by SHA or expected to be implemented by SHA in the near future. See also 2.3.4 I

All costs, including, but not limited to, the actual course costs and course attendance time are the responsibility of the TO Contractor. SHA will not reimburse any costs associated with the professional development of TO Contractor Personnel.

The Offeror shall submit a Professional Development Plan as part of the TO Technical Proposal that identifies both annual training course cost allotments as well as annual training time allotments for all resources planned on this Task Order.

3.11 Substitution of Personnel

3.11.1 Directed Personnel Replacement

A. The TO Manager may direct the TO Contractor to replace any TO Contractor Personnel who, in the sole discretion of the TO Manager, are perceived as being unqualified, non-productive, unable to fully perform the job duties, disruptive, or known, or reasonably believed, to have committed a major infraction(s) of law or Agency, Contract, or Task Order requirement.

B. If deemed appropriate in the discretion of the TO Manager, the TO Manager shall give written notice of any TO Contractor Personnel performance issues to the TO Contractor, describing the problem and delineating the remediation requirement(s). The TO Contractor shall provide a written Remediation Plan within three (3) days of the date of the notice. If the TO Manager rejects the Remediation Plan, the TO Contractor shall revise and resubmit the plan to the TO Manager within five (5) days of the rejection, or in the timeframe set forth by the TO Manager in writing. Once a Remediation Plan has been accepted in writing by the TO Manager, the TO Contractor shall immediately implement the Remediation Plan.

C. Should performance issues persist despite the approved Remediation Plan, the TO Manager will give written notice of the continuing performance issues and either request a new Remediation Plan within a specified time limit or direct the removal and replacement of the TO Contractor Personnel whose performance is at issue. A request for a new Remediation Plan will follow the procedure described in **Section 3.11.1.B**.

D. In circumstances of directed removal, the TO Contractor shall provide a suitable replacement for TO Manager approval within fifteen (15) days of the date of the notification of directed removal, or the actual removal, whichever occurs first, or such earlier time as directed by the TO Manager in the event of a removal on less than fifteen days' notice

E. Normally, a directed personnel replacement will occur only after prior notification of problems with requested remediation, as described above. However, the TO Manager reserves the right to direct immediate personnel replacement without utilizing the remediation procedure described above.

F. Replacement or substitution of TO Contractor Personnel under this section shall be in addition to, and not in lieu of, the State's remedies under the Task Order or which otherwise may be available at law or in equity.

G. All Substitutions of personnel require a Criminal Background Check.

3.11.2 Substitution Prior to and 30 Days After Task Order Execution

A. Prior to Task Order Execution or within thirty (30) days after Task Order Execution, the Offeror may substitute proposed Key Personnel only under the following circumstances: vacancy occurs due to the sudden termination, resignation, or approved leave of absence due to an *Extraordinary Personnel Event*, or death of such personnel. To qualify for such substitution, the Offeror must describe to the State's satisfaction the event necessitating substitution and must demonstrate that the originally proposed personnel are actual full-time direct employees with the Offeror (subcontractors, temporary staff or 1099 contractors do not qualify). Proposed substitutions shall be of equal caliber or higher, in the State's sole discretion. Proposed substitutes deemed by the State to be less qualified than the originally proposed individual may be grounds for pre-award disqualification or post-award termination.

B. An *Extraordinary Personnel Event* – means Leave under the Family Medical Leave Act; an incapacitating injury or incapacitating illness; or other circumstances that in the sole discretion of the State warrant an extended leave of absence, such as extended jury duty or extended military service.

3.11.3 Substitution More Than 30 Days After Task Order Execution

The procedure for substituting personnel after Task Order execution is as follows:

A. The TO Contractor may not substitute personnel without the prior approval of the TO Manager.

B. To replace any personnel, the TO Contractor shall submit resumes of the proposed individual specifying the intended approved labor category. Any proposed substitute personnel shall have qualifications equal to or better than those of the replaced personnel.

C. Proposed substitute individual shall be approved by the TO Manager. The TO Manager shall have the option to interview the proposed substitute personnel and may require that such interviews be in person. After the interview, the TO Manager shall notify the TO Contractor of acceptance or denial of the requested substitution. If no acceptable substitute personnel is proposed within the time frame established by the TO Manager, the TO Agreement may be cancelled. A Criminal Background Check is required.

3.12 Minority Business Enterprise (MBE) Reports

3.12.1 MBE PARTICIPATION REPORTS

Agency will monitor both the TO Contractor's efforts to achieve the MBE participation goal and compliance with reporting requirements.

3.12.2 Monthly reporting of MBE participation is required in accordance with the terms and conditions of the CATS+ Master Contract.

1. The TO Contractor shall submit the following reports by the 15th of each month to the Agency at the same time the invoice copy is sent:

2. A Prime Contractor Paid/Unpaid MBE Invoice Report (**Attachment D MDOT MBE Form D-5**) listing any unpaid invoices, over 45 days old, received from any certified MBE subcontractor, the amount of each invoice and the reason payment has not been made; and

3. (If Applicable) An MBE Prime Contractor Report identifying an MBE prime's self-performing work to be counted towards the MBE participation goals.

3.12.3 The TO Contractor shall ensure that each MBE subcontractor provides a completed Subcontractor Paid/Unpaid MBE Invoice Report (**Attachment D MDOT MBE Form D-6**) by the 15th of each month.

3.12.4 Subcontractor reporting shall be sent directly from the subcontractor to the Agency. The TO Contractor shall e-mail all completed forms, copies of invoices and checks paid to the MBE directly to the TO Manager.

3.13 Veteran Small Business Enterprise (VSBE) Reports

There is no VSBE Goal for this Task Order.

3.14 Work Orders

A. Additional services and resources will be provided via a Work Order process. Work shall not begin in advance of a fully executed Work Order. A Work Order may be issued for time and materials (T&M) or fixed pricing. T&M Work Orders will be issued in accordance with pre-approved Labor Categories with the fully loaded rates proposed in **Attachment B**.

B. The TO Manager shall e-mail a Work Order Request (See sample at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+WorkOrderSample.pdf) to the TO Contractor to provide services or resources that are within the scope of this TORFP. The Work Order Request will include:

1. Technical requirements and description of the service or resources needed
2. Performance objectives and/or deliverables, as applicable
3. Due date and time for submitting a response to the request, and
4. Required place(s) where work must be performed

C. The TO Contractor shall e-mail a response to the TO Manager within the specified time and include at a minimum:

1. A response that details the TO Contractor's understanding of the work;
2. A price to complete the Work Order Request using the format provided (see online sample).
3. A description of proposed resources required to perform the requested tasks, with labor categories listed in accordance with Attachment B.
4. An explanation of how tasks shall be completed. This description shall include proposed subcontractors and related tasks.
5. State-furnished information, work site, and/or access to equipment, facilities, or personnel
6. The proposed personnel resources, including any subcontractor personnel, to complete the task.

D. For a T&M Work Order, the TO Manager will review the response and will confirm the proposed labor rates are consistent with this TORFP. For a fixed price Work Order, the TO Manager will review the response and will confirm the proposed prices are acceptable.

E. The TO Manager may contact the TO Contractor to obtain additional information, clarification or revision to the Work Order, and will provide the Work Order to the TO Procurement Officer for a determination of compliance with the TO Agreement and a determination whether a change order is appropriate. Written TO Procurement Officer approval is required before Work Order execution by the State.

F. Proposed personnel on any type of Work Order shall be subject to Agency approval. The TO Contractor shall furnish resumes of proposed personnel specifying the labor category(ies) proposed.

The TO Manager shall have the option to interview the proposed personnel and, in the event of an interview or not, shall notify the TO Contractor of acceptance or denial of the personnel.

G. Performance of services under a Work Order shall commence consistent with an NTP issued by the TO Manager for such Work Order.

3.15 Additional Clauses

The TO Contractor shall be subject to the requirements in this section and shall flow down the provisions of **Sections 3.15.1 – 3.15.8**(or the substance thereof) in all subcontracts.

3.15.1 TORFP Subject to CATS+ Master Contract

In addition to the requirements of this TORFP, the Master Contractors are subject to all terms and conditions contained in the CATS+ RFP issued by the Maryland Department of Information Technology (DoIT) and subsequent Master Contract Project Number 060B2490023, including any amendments, including but not limited to:

A. Custom Software, Custom Source Code, Data;

B. Hardware and software costs procured as part of the TORFP cannot exceed 49 percent of the total Task Order value;

C. Material costs shall be passed through with no mark-up by the TO Contractor;

D. Non-Visual Access

E. By responding to this TORFP and accepting a Task Order award, an Offeror specifically agrees that for any software, hardware or hosting service that it proposes for use by the State in response to this TORFP, the State will have the right to purchase from another source, instead of from the selected Offeror.

3.15.2 All times specified in this document are local time, defined as Eastern Standard Time or Eastern Daylight Time, whichever is in effect.

3.15.3 Contract Management Oversight Activities

A. DoIT is responsible for contract management oversight on the CATS+ Master Contract. As part of that oversight, DoIT has implemented a process for self-reporting contract management activities of Task Orders under CATS+. This process typically applies to active TOs for operations and maintenance services valued at $1 million or greater, but all CATS+ Task Orders are subject to review.

B. A sample of the TO Contractor Self-Reporting Checklist is available on the CATS+ website at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+Self-ReportingChecklistSample.pdf. DoIT may send initial checklists out to applicable/selected TO Contractors approximately three months after the award date for a Task Orders. The TO Contractor shall complete and return the checklist as instructed on the form. Subsequently, at six-month intervals from the due date on the initial checklist, the TO Contractor shall update and resend the checklist to DoIT.

3.15.4 Source Code Escrow

Source code Escrow does not apply to this Task Order.

3.15.5 Purchasing and Recycling Electronic Products

This section does not apply to this solicitation.

3.15.6 Change Control and Advance Notice

This section does not apply to this solicitation.

3.15.7 No-Cost Extensions

In the event there are unspent funds remaining on the TO Agreement, prior to the TO's expiration date the TO Procurement Officer may modify the TO Agreement to extend the TO Agreement beyond its expiration date for the performance of work within the TO's scope of work. Notwithstanding anything to the contrary, no funds may be added to the TO Agreement in connection with any such extension.

3.15.8 CERTIFICATION REGARDING DISCRIMINATORY BOYCOTTS OF ISRAEL

TO Proposals must contain a completed certification (Appendix 7) that the Master Contractor: (1) is not engaging in a boycott of Israel and that (2) it will, for the duration of its contractual obligations, refrain from a boycott of Israel.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

4 TORFP Instructions

4.1 TO Pre-Proposal Conference

4.1.1 A TO pre-proposal conference (Conference) will be held at the date, time, and location indicated on the Key Information Summary Sheet.

4.1.2 Attendance at the Conference is not mandatory, but all interested parties are encouraged to attend in order to facilitate better preparation of their proposals.

4.1.3 Following the Conference, the attendance record and summary of the Conference will be distributed via e-mail to all Master Contractors known to have received a copy of this TORFP.

4.1.4 Attendees should bring a copy of the solicitation and a business card to help facilitate the sign-in process.

4.1.5 In order to assure adequate seating and other accommodations at the Conference, please e-mail the Pre-Proposal Conference Response Form (**Attachment A**) no later than the time and date indicated on the form. In addition, if there is a need for sign language interpretation and/or other special accommodations due to a disability, please notify the TO Procurement Officer at least five (5) business days prior to the Conference date. The Agency will make a reasonable effort to provide such special accommodation.

4.1.6 Seating at the Conference will be limited to two (2) attendees per company.

4.2 Questions

4.2.1 All questions shall identify in the subject line the Solicitation Number and Title (J02B8400024 - SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP), and shall be submitted in writing via e-mail to the TO Procurement Officer no later than the date and time specified the Key Information Summary Sheet.

4.2.2 Answers to all questions that are not clearly specific only to the requestor will be provided to all Master Contractors who are known to have received a copy of the TORFP.

4.2.3 The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Agency unless it issues an amendment in writing.

4.3 TO Proposal Due (Closing) Date and Time

4.3.1 TO Proposals, in the number and form set forth in **Section 5 TO Proposal Format**, must be received by the TO Procurement Officer no later than the TO Proposal due date and time indicated on the Key Information Summary Sheet in order to be considered.

4.3.2 Requests for extension of this date or time shall not be granted.

4.3.3 Offerors submitting TO Proposals should allow sufficient delivery time to ensure timely receipt by the TO Procurement Officer. Except as provided in COMAR 21.05.03.02.F and 21.05.02.10, TO Proposals received after the due date and time listed in the Key Information Summary Sheet will not be considered.

4.3.4 The date and time of an e-mail submission is determined by the date and time of arrival in the e-mail address indicated on the Key Information Summary Sheet.

4.3.5 TO Proposals may be modified or withdrawn by written notice received by the TO Procurement Officer before the time and date set forth in the Key Information Summary Sheet for receipt of TO Proposals.

4.4 Award Basis

Based upon an evaluation of TO Proposal responses as provided in **Section 6.4**, below, a Master Contractor will be selected to conduct the work defined in **Sections 2** and **3**. A specific TO Agreement, **Attachment M**, will then be entered into between the State and the selected Master Contractor, which will bind the selected Master Contractor (TO Contractor) to the contents of its TO Proposal, including the TO Financial Proposal.

4.5 Oral Presentation

4.5.1 Offerors and proposed TO Contractor Personnel will be required to make an oral presentation to State representatives. Offerors must confirm in writing any substantive oral clarification of, or change in, their Proposals made in the course of discussions. Any such written clarifications or changes then become part of the Master Contractor's TO Proposal. The TO Procurement Officer will notify Offerors of the time and place of oral presentations and interviews, should interviews be scheduled separately.

4.5.2 All proposed personnel for Offerors meeting minimum qualifications shall participate in interviews, which are a type of oral presentation. All candidates shall be interviewed in substantially the same manner. The TO Procurement Officer shall, for each round of interviews, determine whether phone or in-person interviews will be utilized. At the TO Procurement Officer's discretion, interviews may be conducted via the internet (e.g., Skype, GotoMeeting, WebEx) in lieu of in-person interviews.

4.6 Limitation of Liability

The TO Contractor's liability is limited in accordance with the Limitations of Liability section of the CATS+ Master Contract. TO Contractor's liability for this TORFP is limited to One (1) times the total TO Agreement amount.

4.7 MBE Participation Goal

4.7.1 A Master Contractor that responds to this TORFP shall complete, sign, and submit all required MBE documentation at the time of TO Proposal submission (See **Attachment D** Minority Business Enterprise Forms). **Failure of the Master Contractor to complete, sign, and submit all required MBE documentation at the time of TO Proposal submission will result in the State's rejection of the Master Contractor's TO Proposal.**

4.7.2 In 2014, Maryland adopted new regulations as part of its Minority Business Enterprise (MBE) program concerning MBE primes. Those new regulations, which became effective June 9, 2014 and are being applied to this task order, provide that when a certified MBE firm participates as a prime contractor on a contract, an agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own forces toward fulfilling up to fifty-percent (50%) of the MBE participation goal (overall) and up to one hundred percent (100%) of not more than one of the MBE participation sub-goals, if any, established for the contract. Please see the attached MBE forms and instructions.

4.8 VSBE Goal

There is no VSBE participation goal for this procurement.

4.9 Living Wage Requirements

The Master Contractor shall abide by the Living Wage requirements under Title 18, State Finance and Procurement Article, Annotated Code of Maryland and the regulations proposed by the Commissioner of Labor and Industry.

All TO Proposals shall be accompanied by a completed Living Wage Affidavit of Agreement, **Attachment F** of this TORFP.

4.10 Federal Funding Acknowledgement

This Task Order does not contain federal funds.

4.11 Conflict of Interest Affidavit and Disclosure

4.11.1 Offerors shall complete and sign the Conflict of Interest Affidavit and Disclosure (**Attachment H**) and submit it with their Proposals. All Offerors are advised that if a TO Agreement is awarded as a result of this solicitation, the TO Contractor's Personnel who perform or control work under this TO Agreement and each of the participating subcontractor personnel who perform or control work under this TO Agreement shall be required to complete agreements substantially similar to **Attachment H**, conflict of interest Affidavit and Disclosure.

4.11.2 If the TO Procurement Officer makes a determination that facts or circumstances exist that give rise to or could in the future give rise to a conflict of interest within the meaning of COMAR 21.05.08.08A, the TO Procurement Officer may reject an Offeror's TO Proposal under COMAR 21.06.02.03B.

4.11.3 Master Contractors should be aware that the State Ethics Law, Md. Code Ann., General Provisions Article, Title 5, might limit the selected Master Contractor's ability to participate in future related procurements, depending upon specific circumstances.

4.11.4 By submitting a Conflict of Interest Affidavit and Disclosure, the Offeror shall be construed as certifying all TO Contractor Personnel and Subcontractors are also without a conflict of interest as defined in COMAR 21.05.08.08A.

4.12 Non-Disclosure Agreement

4.12.1 Non-Disclosure Agreement (Offeror)

A Non-Disclosure Agreement (Offeror) is not required for this solicitation.

4.12.2 Non-Disclosure Agreement (TO Contractor)

All Offerors are advised that this solicitation and any TO Agreement(s) are subject to the terms of the Non-Disclosure Agreement (NDA) contained in this solicitation as **Attachment I**. This Agreement must be provided within five (5) Business Days of notification of recommended award; however, to expedite processing, it is suggested that this document be completed and submitted with the TO Proposal.

4.13 HIPAA - Business Associate Agreement

A HIPAA Business Associate Agreement is not required for this procurement.

4.14 Iranian Non-Investment

All TO Proposals shall be accompanied by a completed Certification Regarding Investments in Iran, **Attachment N** of this TORFP.

4.15 Mercury and Products That Contain Mercury

This solicitation does not include the procurement of products known to likely include mercury as a component.

4.16 Location of the Performance of Services Disclosure

The Offeror is required to complete the Location of the Performance of Services Disclosure. A copy of this Disclosure is included as **Attachment L**. The Disclosure must be provided with the TO Proposal.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

5 TO Proposal Format

5.1 Required Response

Each Master Contractor receiving this CAT+ TORFP shall respond no later than the submission due date and time designated in the Key Information Summary Sheet or as amended. Each Master Contractor is required to submit one of two possible responses: 1) a TO Proposal; or 2) a completed Master Contractor Feedback Form (available online within the Master Contractor Admin System). The feedback form helps the State understand for future contract development why Master Contractors did not submit proposals. The form is accessible via the CATS+ Master Contractor login screen and clicking on TORFP Feedback Response Form from the menu.

A TO Proposal shall conform to the requirements of this CATS+ TORFP.

5.2 Two Part Submission

Offerors shall submit TO Proposals in separate volumes:

- Volume I – TO TECHNICAL PROPOSAL
- Volume II – TO FINANCIAL PROPOSAL

5.3 TO Proposal Packaging and Delivery

5.3.1 TO Proposals delivered by facsimile shall not be considered.

5.3.2 Provide no pricing information in the TO Technical Proposal. Provide no pricing information on the media submitted in the TO Technical Proposal.

5.3.3 Offerors may submit TO Proposals by electronic means as described.

A. Electronic means includes e-mail to the TO Procurement Officer address listed on the Key Information Summary Sheet.

B. An Offeror wishing to deliver a hard copy (paper) TO Proposal shall contact the TO Procurement Officer for instructions.

5.3.4 E-mail submissions

A. All TO Proposal e-mails shall be sent with password protection.

B. The TO Procurement Officer will not accept submissions after the date and exact time stated in the Key Information Summary Sheet. The date and time of submission is determined by the date and time of arrival in the TO Procurement Officer's e-mail box. Time stamps on outgoing email from Master TO Contractors shall not be accepted. Requests for extension of this date or time will not be granted. Except as provided in COMAR 21.05.03.02F, TO Proposals received by the TO Procurement Officer after the due date will not be considered.

C. The State has established the following procedure to restrict access to TO Proposals received electronically: all Technical and TO Financial Proposals must be password protected, and the password for the TO TECHNICAL PROPOSAL must be different from the password for the TO Financial Proposal. Offerors will provide these two passwords to SHA upon request or their TO Proposal will be deemed not susceptible for award. Subsequent submissions of TO Proposal content will not be allowed.

D. The TO Procurement Officer will only contact those Offerors with TO Proposals that are reasonably susceptible for award.

E. TO Proposals submitted via e-mail must not exceed 7 Mb. If a submission exceeds this size, split the submission into two or more parts and include the appropriate part number in the subject (e.g., part 1 of 2) after the subject line information below.

F. The e-mail submission subject line shall state the TORFP J02B8400024 and either "Technical" or "Financial."

5.3.5 Two Part Submission:

A. TO Technical Proposal consisting of:

1. TO Technical Proposal and all supporting material in Microsoft Word format, version 2007 or greater,

2. the TO Technical Proposal in searchable Adobe PDF format,

3. a second searchable Adobe copy of the TO Technical Proposal, redacted in accordance with confidential and/or proprietary information removed (see **Section 5.4.2.B**, and

B. TO Financial Proposal consisting of:

1. TO Financial Proposal and all supporting material in Word format,

2. the TO Financial Proposal in searchable Adobe PDF format,

3. a second searchable Adobe copy of the TO Financial Proposal, redacted in accordance with confidential and/or proprietary information removed (see **Section 5.4.2.B**).

5.4 Volume I - TO Technical Proposal

NOTE: Provide **no pricing information** in the TO Technical Proposal (Volume I). Include pricing information only in the TO Financial Proposal (Volume II).

5.4.1 In addition to the instructions below, responses in the Offeror's TO Technical Proposal shall reference the organization and numbering of Sections in the TORFP (e.g., "Section 2.2.1 Response . . .; "Section 2.2.2 Response . . .,"). All pages of both TO Proposal volumes shall be consecutively numbered from beginning (Page 1) to end (Page "x").

5.4.2 The TO Technical Proposal shall include the following documents and information in the order specified as follows:

A. Proposed Services:

1. Executive Summary: A one-page summary describing the Offeror's understanding of the TORFP scope of work (**Sections 2-3**) and proposed solution.

2. Proposed Solution: A more detailed description of the Offeror's understanding of the TORFP scope of work, proposed methodology and solution. The proposed solution shall be organized to exactly match the requirements outlined in Sections 2-3.

3. Professional Development Plan: Provide a summary on the importance of technical training and how the Offeror promotes it. Detail the annual allotted costs per resource in both course fees and time that will elevate their skill set per Section 2.3.4.I. Also detail any training options provided by the Offeror that are available to the resources.

B. Proposer Information Sheet and Transmittal Letter

The Offeror Information Sheet (see **Appendix 2**) and a Transmittal Letter shall accompany the TO Technical Proposal. The purpose of the Transmittal Letter is to transmit the TO Proposal and acknowledge the receipt of any addenda to this TORFP issued before the TO

Proposal due date and time. Transmittal Letter should be brief, be signed by an individual who is authorized to commit the Offeror to its TO Proposal and the requirements as stated in this TORFP and contain acknowledgement of all addenda to this TORFP issued before the TO Proposal due date.

C. Minimum Qualifications Documentation (If applicable)

Offeror company minimum qualifications do not apply to this TORFP.

D. Proposed Personnel and TORFP Staffing

Offeror shall propose exactly four (4) Key Personnel in response to this TORFP. Offeror shall:

1. Identify the qualifications and types of staff proposed to be utilized under the Task Order. The Offeror shall describe in detail how the proposed staff's experience and qualifications relate to their specific responsibilities, including any staff of proposed subcontractor(s), as detailed in the Work Plan.
2. Complete and provide for each proposed resource **Appendix 3A** Minimum Qualifications Summary and **Appendix 3B** Personnel Resume Form.
3. Provide evidence proposed personnel possess the required certifications in accordance with **Section 1.1** Offeror Personnel Minimum Qualifications. Also provide any specific proof requirements such as an image of the proposed personnel's unexpired certifications.
4. Provide three (3) references per proposed Key Personnel containing the information listed in **Appendix 3B**.
5. Provide a Staffing Management Plan that demonstrates how the Offeror will provide all planned resources (see Section 2.3.6 Number of Personnel to Propose) in addition to the four (4) Key personnel requested in this TORFP, and how the TO Contractor Personnel shall be managed. Include:
   a) Planned team composition by role (**Important! Identify specific names and provide history only for the proposed resources required for evaluation of this TORFP**).
   b) Process and proposed lead time for locating and bringing on board resources that meet the Task Order needs.
   c) Supporting descriptions for all labor categories proposed in response to this TORFP.
   d) Description of approach for quickly substituting qualified personnel after start of the Task Order.
6. Provide the names and titles of the Offeror's management staff who will supervise the personnel and quality of services rendered under this TO Agreement.

E. Subcontractors

Identify all proposed Subcontractors, including MBEs, and their roles in the performance of the scope of work hereunder.

F. Overall Offeror team organizational chart

Provide an overall team organizational chart with all team resources available to fulfill the Task Order scope of work.

G. Master Contractor and Subcontractor Experience and Capabilities

1. Provide up to three examples of engagements or contracts the Master Contractor or Subcontractor, if applicable, has completed that were similar to the requested scope of work. Include contact information for each client organization complete with the following:

   a) Name of organization.

   b) Point of contact name, title, e-mail and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

   c) Services provided as they relate to the scope of work.

   d) Start and end dates for each example engagement or contract.

   e) Current Master Contractor team personnel who participated on the engagement.

   f) If the Master Contractor is no longer providing the services, explain why not.

2. State of Maryland Experience: If applicable, the Master Contractor shall submit a list of all contracts it currently holds or has held within the past five years with any entity of the State of Maryland.

   For each identified contract, the Master Contractor shall provide the following (if not already provided in sub paragraph A above):

   a) Contract or task order name

   b) Name of organization.

   c) Point of contact name, title, e-mail, and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

   d) Start and end dates for each engagement or contract. If the Master Contractor is no longer providing the services, explain why not.

   e) Dollar value of the contract.

   f) Indicate if the contract was terminated before the original expiration date.

   g) Indicate if any renewal options were not exercised.

Note - State of Maryland experience can be included as part of **G.1** above as engagement or contract experience. State of Maryland experience is neither required nor given more weight in proposal evaluations.

H. State Assistance

Provide an estimate of expectation concerning participation by State personnel.

I. Confidentiality

A Master Contractor should give specific attention to the identification of those portions of its proposal that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Public Information Act, Title 4, of the General Provisions Article of the Annotated Code of Maryland. Master Contractors are advised

that, upon request for this information from a third party, the TO Procurement Officer will be required to make an independent determination regarding whether the information may be disclosed.

Offeror shall furnish a list that identifies each section of the TO Technical Proposal where, in the Offeror's opinion, the Offeror's response should not be disclosed by the State under the Public Information Act.

J. Additional Submissions:

1. Attachments and Exhibits;

a) All forms required for the TO Technical Proposal are identified in **Table 1 of Section 7** – Exhibits and Attachments. Unless directed otherwise by instructions within an individual form, complete, sign, and include all required forms in the TO Technical Proposal.

b) No attachment forms shall be altered. Signatures shall be clearly visible.

5.5 Volume II – TO Financial Proposal

5.5.1 The TO Financial Proposal shall contain all price information in the format specified in **Attachment B -** Financial Proposal Form. The Offeror shall complete the Financial Proposal Form only as provided in the Financial Proposal Form Instructions and the Financial Proposal Form itself.

5.5.2 The TO Financial Proposal shall contain a description of any assumptions on which the Master Contractor's TO Financial Proposal is based (Assumptions shall not constitute conditions, contingencies, or exceptions to the Financial Proposal Form);

5.5.3 **Attachment B**– Financial Proposal Form, with all proposed labor categories including all rates fully loaded. Master Contractors shall list all key resources by approved CATS+ labor categories in the TO Financial Proposal.

5.5.4 To be responsive to this TORFP, the Financial Proposal Form shall provide labor rates for all labor categories anticipated for this TORFP. Proposed rates shall not exceed the rates defined in the Master Contract for the Master Contract year(s) in effect at the time of the TO Proposal due date.

5.5.5 **Note: Failure to specify a CATS+ labor category in the completed Financial Proposal Form for each proposed resource will make the TO Proposal non-responsive to this TORFP.**

5.5.6 Prices shall be valid for 120 days.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

6 Evaluation and Selection Process

The TO Contractor will be selected from among all eligible Master Contractors within the appropriate Functional Area responding to the CATS+ TORFP. In making the TO Agreement award determination, the Agency will consider all information submitted in accordance with Section 5.

6.1 Evaluation Committee

Evaluation of TO Proposals will be performed in accordance with COMAR 21.05.03 by a committee established for that purpose and based on the evaluation criteria set forth below. The Evaluation Committee will review TO Proposals, participate in Offeror oral presentations and discussions, and provide input to the TO Procurement Officer. The Agency reserves the right to utilize the services of individuals outside of the established Evaluation Committee for advice and assistance, as deemed appropriate.

During the evaluation process, the TO Procurement Officer may determine at any time that a particular Offeror is not susceptible for award.

6.2 TO Technical Proposal Evaluation Criteria

The criteria to be used to evaluate each TO Technical Proposal are listed below in descending order of importance. Unless stated otherwise, any sub-criteria within each criterion have equal weight.

6.2.1 Offeror's Technical Response to TORFP Requirements (See TORFP **§ 5.4.2**)

The State prefers an Offeror's response to work requirements in the TORFP that illustrates a comprehensive understanding of work requirements and mastery of the subject matter, including an explanation of how the work will be performed. TO Proposals which include limited responses to work requirements such as "concur" or "will comply" will receive a lower ranking than those TO proposals that demonstrate an understanding of the work requirements and include plans to meet or exceed them.

6.2.2 Experience and Qualifications of Proposed Staff (See TORFP **§ 5.4.2.D**)

The capability of the proposed resources to perform the required tasks and produce the required deliverables in the TORFP **Sections 2-3**. Capability will be determined from each proposed individual's resume, reference checks, and oral presentation (See **Section 4.5** Oral Presentation).

6.2.3 Offeror Qualifications and Capabilities, including proposed subcontractors (See TORFP **§** 5.4.2.G)

a. The State prefers an Offeror's response to its qualifications and capabilities that include specifically programmer experience with the multiple programming languages as specified in Section 2.3.6.

b. References able to attest to the Offeror's experience with staffing contracts for projects and/or services as referenced in the TORFP.

6.2.4 Demonstration of how the Master Contractor plans to staff the task order at the levels set forth in the TORFP and also for potential future resource requests.

6.2.5 Response to the Professional Development Plan as specified in Section 3.10.11, 2.3.4 I.

6.3 TO Financial Proposal Evaluation Criteria

All Qualified Offerors (see **Section 6.4**) will be ranked from the lowest (most advantageous) to the highest (least advantageous) price based on the Total Proposal Price within the stated guidelines set forth in this TORFP and as submitted on **Attachment B** - TO Financial Proposal Form.

6.4 Selection Procedures

TO Technical Proposals shall be evaluated based on the criteria set forth above in **Section 6.2**. TO Technical Proposals and TO Financial Proposals will be evaluated independently of each other.

A. TO Proposals will be assessed throughout the evaluation process for compliance with the minimum qualifications listed in Section 1 of this TORFP, and quality of responses to **Section 5.3** TO Technical Proposal. Failure to meet the minimum qualifications shall render a TO Proposal not reasonably susceptible for award. The TO Procurement Officer will notify those Offerors who have not been selected to perform the work.

B. TO Technical Proposals will be evaluated for technical merit and ranked. At the State's sole discretion, a down-select procedure may be followed as described in 6.4.1 below. Oral presentations and discussions may be held to assure full understanding of the State's requirements and of the qualified Offeror's proposals and abilities to perform, and to facilitate arrival at a TO Agreement that is most advantageous to the State.

C. The Procurement Officer will only open the TO Financial Proposals where the associated TO Technical Proposals have been classified as reasonably susceptible for award.

D. After review of TO Financial Proposals, TO Financial Proposals for qualified Offerors will be reviewed and ranked from lowest to highest price proposed.

E. When in the best interest of the State, the TO Procurement Officer may permit Qualified Offerors to revise their initial Proposals and submit, in writing, Best and Final Offers (BAFOs). The State may make an award without issuing a request for a BAFO.

F. The Procurement Officer shall make a determination recommending award of the TO to the responsible Offeror who has the TO Proposal determined to be the most advantageous to the State, considering price and the evaluation criteria set forth above. In making this selection, the TO Technical Proposal will be given greater weight than the TO Financial Proposal.

All Master Contractors submitting a TO Proposal shall receive written notice from the TO Procurement Officer identifying the awardee.

6.4.1 Down-Select Procedure

In the event that more than ten (10) qualified TO Proposals are received, the TO Procurement Officer may elect to follow a down-select process as follows:

A. A technical ranking will be performed for all TO Proposals based on the resumes submitted. TO Proposals will be ranked from highest to lowest for technical merit based on the quality of the resumes submitted and the extent to which the proposed individuals' qualifications align with the position needs as described in this TORFP.

B. The top ten (10) TO Proposals identified by the technical ranking will be invited to interviews. All other Offerors will be notified of non-selection for this TORFP.

6.5 Documents Required upon Notice of Recommendation for Task Order Award

Upon receipt of a Notification of Recommendation for Task Order award, the apparent awardee shall complete and furnish the documents and attestations as directed in Table 1 of **Section 7 – TORFP Attachments and Appendices**.

Commencement of work in response to a TO Agreement shall be initiated only upon the completed documents and attestations, plus:

A. Issuance of a fully executed TO Agreement,

B. Purchase Order, and

C. by a Notice to Proceed authorized by the TO Manager. See (see online example at http://doit.maryland.gov/contracts/Documents/CATSPlus/CATS+NoticeToProceedSample.pdf).

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

7 TORFP ATTACHMENTS AND APPENDICES

Instructions Page

A TO Proposal submitted by an Offeror must be accompanied by the completed forms and/or affidavits identified as "with proposal" in the "When to Submit" column in Table 1 below. All forms and affidavits applicable to this TORFP, including any applicable instructions and/or terms, are identified in the "Applies" and "Label" columns in Table 1.

For documents required as part of the proposal:

A. For e-mail submissions, submit one (1) copy of each with signatures.

B. For paper submissions, submit two (2) copies of each with original signatures. All signatures must be clearly visible.

All Offerors are advised that if a Task Order is awarded as a result of this solicitation, the successful Offeror will be required to complete certain forms and affidavits after notification of recommended award. The list of forms and affidavits that must be provided is described in Table 1 below in the "When to Submit" column.

For documents required after award, submit three (3) copies of each document within the appropriate number of days after notification of recommended award, as listed in Table 1 below in the "When to Submit" column.

Table 1: TORFP ATTACHMENTS AND APPENDICES

Applies?	When to Submit	Label	Attachment Name
Y	Before TO Proposal	A	Pre-Proposal Conference Response Form
Y	With TO Proposal	B	TO Financial Proposal Instructions and Form
N	n/a	C	RESERVED
Y	With TO Proposal	D	MDOT MBE Forms A and B **Important:** MDOT MBE Form E, if a waiver has been requested, is also required with TO Proposal
Y	Within 10 days after recommended award	D	MDOT MBE Forms C and D
Y	As directed in forms	D	MDOT MBE Forms D-5 and D-6
N	With TO Proposal	E	Veteran-Owned Small Business Enterprise (VSBE) Form E-1
N	5 Business Days after recommended award	E	VSBE Forms E-1B, E-2, E-3
Y	With TO Proposal	F	Maryland Living Wage Requirements for Service Task Orders and Affidavit of Agreement
N	With TO Proposal	G	Federal Funds Attachments
Y	With TO Proposal	H	Conflict of Interest Affidavit and Disclosure

Applies?	When to Submit	Label	Attachment Name
Y	5 Business Days after recommended award	I	Non-Disclosure Agreement (TO Contractor)
N	5 Business Days after recommended award	J	HIPAA Business Associate Agreement
N	With TO Proposal	K	Mercury Affidavit
Y	With TO Proposal	L	Location of the Performance of Services Disclosure
Y	5 Business Days after recommended award	M	Task Order Agreement
Y	With TO Proposal	N	Certification regarding Investments in Iran

Appendices

Applies?	When to Submit	Label	Attachment Name
Y	N/A	1	Abbreviations and Definitions
Y	With TO Proposal	2	Offeror Information Sheet
Y	With TO Proposal	3	Labor Classification Personnel Resume Summary (Appendix 3A and 3B)
Y	Within 30 days after NTP Date	4	Criminal Background Check Affidavit
Y	N/A	5	Maryland Department of Transportation Information Security Policy
Y	After NTP Date	6	Weekly TO Contract Personnel Status Report
Y	With TO Proposal	8	Certification Regarding Discriminatory Boycotts of Israel

Additional Submissions

Applies?	When to Submit	Label	Attachment Name
Y	5 Business Days after recommended award	--	Evidence of meeting insurance requirements (see **Section 3.6**); 1 copy

Attachment A. TO Pre-Proposal Conference Response Form

Solicitation Number J02B8400024

SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP

A TO Pre-proposal conference will be held on Wednesday, 4/11/2018 at 10:00 AM -11:30 AM (EST), at Maryland Department of Transportation, TSO, 4th Floor Board Room.

Please return this form

to Peggy Tischler at ptischler@mdot.state.md.us no later than 2:00 PM on Monday, 4/9/2018 by close of business advising whether or not you plan to attend. The completed form should be returned via e-mail or fax to the Procurement Officer at the contact information below:

Peggy Tischler

MDOT
E-mail: ptischler@mdot.state.md.us;
Fax #: 410-865-1388

Please indicate:

_____ Yes, the following representatives will be in attendance.
Attendees (attendance is limited to 2 attendees from each Firm):
1.

2.

_____ No, we will not be in attendance.

Please specify whether any reasonable accommodations are requested (see TORFP § 4.1"TO Pre-proposal conference"):

Offeror: _____
Offeror Name (please print or type)

By: _____
Signature/Seal

Printed Name: _____
Printed Name

Title: _____
Title

Date: _____
Date

DIRECTIONS TO THE TO PRE-PROPOSAL CONFERENCE

Maryland Department of Transportation
Headquarters
7201 Corporate Center Drive
Hanover MD 21076
410-865-1000
Toll Free 1-888-713-1414

From the South
From I-97 take MD 100 West to MD 170 North. Take MD 170 North to Stoney Run. Take the ramp that veers to the right. Make a left at the top of the ramp and cross over MD 170. Proceed to the next light this will be the New Ridge Road intersection, turn right Corporate Center Drive begins. MDOT Headquarters is ¾ mile on the right side of the road. Visitor parking is to the left.

From the North
From I-95 or BW Parkway take I-195 to MD 170 South to Stoney Run. Turn left at the light. Make a left at the top of the ramp and cross over MD 170. Proceed to the next light this will be the New Ridge Road intersection, turn right Corporate Center Drive begins. MDOT Headquarters is ¾ mile on the right side of the road. Visitor parking is to the left.

Marc Train Service
Ride the Marc Penn Line Train from both the South and North and exit at the BWI Marc Train Station. When you exit the train follow directions to the crossover (tracks) and you will find an exit door on the second floor leading to a pedestrian bridge. This pedestrian bridge will carry you (1600 ft.) to MDOT

Light Rail Service
Ride the light rail from the North to the BWI Airport Station. There is shuttle service from the BWI Airport to BWI Marc Train Station. Take the crossover (tracks) and on the second floor there is an exit to the Pedestrian Bridge for MDOT. This pedestrian bridge will carry you (1600 ft.) to MDOT

Attachment B. TO Financial Proposal Instructions & Form

B-1 FINANCIAL PROPOSAL INSTRUCTIONS

In order to assist Offerors in the preparation of their Financial Proposal and to comply with the requirements of this solicitation, Financial Proposal Instructions and a Financial Proposal Form have been prepared. Offerors shall submit their Financial Proposal on the Financial Proposal Form in accordance with the instructions on the Financial Proposal Form and as specified herein. Do not alter the Financial Proposal Form or the Proposal may be determined to be not reasonably susceptible of being selected for award. The Financial Proposal Form is to be signed and dated, where requested, by an individual who is authorized to bind the Offeror to the prices entered on the Financial Proposal Form.

The Financial Proposal Form is used to calculate the Offeror's TOTAL PROPOSAL PRICE. Follow these instructions carefully when completing your Financial Proposal Form:

A) All Unit and Extended Prices must be clearly entered in dollars and cents, e.g., $24.15. Make your decimal points clear and distinct.

B) All Unit Prices must be the actual price per unit the State will pay for the specific item or service identified in this RFP and may not be contingent on any other factor or condition in any manner.

C) All calculations shall be rounded to the nearest cent, i.e., .344 shall be .34 and .345 shall be .35.

D) Any goods or services required through this TORFP and proposed by the vendor at No Cost to the State must be clearly entered in the Unit Price, if appropriate, and Extended Price with $0.00.

E) Every blank in every Financial Proposal Form shall be filled in. Any changes or corrections made to the Financial Proposal Form by the Offeror prior to submission shall be initialed and dated.

F) Except as instructed on the Financial Proposal Form, nothing shall be entered on or attached to the Financial Proposal Form that alters or proposes conditions or contingencies on the prices. Alterations and/or conditions may render the Proposal not reasonably susceptible of being selected for award.

G) It is imperative that the prices included on the Financial Proposal Form have been entered correctly and calculated accurately by the Offeror and that the respective total prices agree with the entries on the Financial Proposal Form. Any incorrect entries or inaccurate calculations by the Offeror will be treated as provided in COMAR 21.05.03.03, and may cause the Proposal to be rejected.

H) If option years are included, Offerors must submit pricing for each option year. Any option to renew will be exercised at the sole discretion of the State and comply with all terms and conditions in force at the time the option is exercised. If exercised, the option period shall be for a period identified in the TORFP at the prices entered in the Financial Proposal Form.

I) All Financial Proposal prices entered below are to be fully loaded prices that include all costs/expenses and/or fees associated with the provision of services as required by the RFP. The Financial Proposal price shall include, but is not limited to, all: labor, profit/overhead, general operating, administrative, and all other expenses and costs necessary to perform the work set forth in the solicitation. No other amounts will be paid to the Contractor. If labor rates are requested, those amounts shall be fully-loaded rates; no overtime amounts will be paid.

J) Unless indicated elsewhere in the TORFP, sample amounts used for calculations on the Financial Proposal Form are typically estimates for evaluation purposes only. Unless stated otherwise in the

TORFP, the Department does not guarantee a minimum or maximum number of units or usage in the performance of this Contract.

K) Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

Attachment B -1 - TO Financial Proposal Instructions & Form - REVISED

The total class hours (Column B) are not to be construed as "guaranteed" hours; the total number of hours is an estimate only for purposes of price sheet evaluation.

A year for this Task Order shall be calculated as one calendar year from the Effective Date. **Labor Rate Maximums:** The maximum labor rate that may be proposed for any CATS+ Labor Category shall not exceed the maximum for the CATS+ Master Contract year in effect on the TO Proposal due date.

Job Title from TORFP	CATS+ Labor Category ***To Be Proposed by Master Contractor**	Hourly Labor Rate (A)	Total Class Hours (B)	Proposal Price (C)
Year 1				
Senior C# .NET Programmer (4 personnel)	Insert CATS+ Labor Category	$	1960	**$**
C# .NET Programmer (8 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
			Evaluated Price Year 1	**$**
Year 2				
Senior C# .NET Programmer (4 personnel)	Insert CATS+ Labor Category	$	1960	**$**
C# .NET Programmer (8 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior PowerBuilder Programmer (1personnel)	Insert CATS+ Labor Category	$	1960	**$**
PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
			Evaluated Price Year 2	**$**
Year 3				
Senior C# .NET Programmer (4 personnel)	Insert CATS+ Labor Category	$	1960	**$**

Job Title from TORFP	CATS+ Labor Category ***To Be Proposed by Master Contractor**	Hourly Labor Rate (A)	Total Class Hours (B)	Proposal Price (C)
C# .NET Programmer (8 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
			Evaluated Price Year 3	**$**
Year 4				
Senior C# .NET Programmer (4 personnel)	Insert CATS+ Labor Category	$	1960	**$**
C# .NET Programmer (8 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
			Evaluated Price Year 4	**$**
Year 5				
Senior C# .NET Programmer (4 personnel)	Insert CATS+ Labor Category	$	1960	**$**
C# .NET Programmer (8 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
SalesForce.com Programmer (2 personnel)	Insert CATS+ Labor Category	$	1960	**$**
Senior PowerBuilder Programmer (1personnel)	Insert CATS+ Labor Category	$	1960	**$**
PowerBuilder Programmer (1 personnel)	Insert CATS+ Labor Category	$	1960	**$**
			Evaluated Price Year 5	**$**

Job Title from TORFP	CATS+ Labor Category ***To Be Proposed by Master Contractor**	Hourly Labor Rate (A)	Total Class Hours (B)	Proposal Price (C)
			Total Proposal Price (year 1 + year 2 + year 3 + year 4 + year 5)	**$**

Authorized Individual Name	Company Name
Title	Company Tax ID #
Signature	Date

The Hourly Labor Rate is the actual rate the State will pay for services and shall be recorded in dollars and cents. The Hourly Labor Rate cannot exceed the Master Contract Rate but may be lower. Rates shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TO Agreement

Attachment C. RESERVED

Attachment D. Minority Business Enterprise (MBE) Forms

TO CONTRACTOR MINORITY BUSINESS ENTERPRISE REPORTING REQUIREMENTS

CATS+ TORFP #J02B8400024

These instructions are meant to accompany the customized reporting forms sent to you by the TO Manager. If, after reading these instructions, you have additional questions or need further clarification, please contact the TO Manager immediately.

1. As the TO Contractor, you have entered into a TO Agreement with the State of Maryland. As such, your company/firm is responsible for successful completion of all deliverables under the contract, including your commitment to making a good faith effort to meet the MBE participation goal(s) established for TORFP. Part of that effort, as outlined in the TORFP, includes submission of monthly reports to the State regarding the previous month's MBE payment activity. Reporting forms D-5 (TO Contractor Paid/Unpaid MBE Invoice Report) and D-6 (Subcontractor Paid/Unpaid MBE Invoice Report) are attached for your use and convenience.

2. The TO Contractor must complete a separate Form D-5 (TO Contractor Paid/Unpaid MBE Invoice Report) for each MBE subcontractor for each month of the contract and submit one copy to each of the locations indicated at the bottom of the form. The report is due no later than the 15th of the month following the month that is being reported. For example, the report for January's activity is due no later than the 15th of February. With the approval of the TO Manager, the report may be submitted electronically. Note: Reports are required to be submitted each month, regardless of whether there was any MBE payment activity for the reporting month.

3. The TO Contractor is responsible for ensuring that each subcontractor receives a copy (e-copy of and/or hard copy) of Form D-6 (Subcontractor Paid/Unpaid MBE Invoice Report). The TO Contractor should make sure that the subcontractor receives all the information necessary to complete the form properly, i.e., all of the information located in the upper right corner of the form. It may be wise to customize Form D-6 (upper right corner of the form) for the subcontractor the same as the Form D-5 was customized by the TO Manager for the benefit of the TO Contractor. This will help to minimize any confusion for those who receive and review the reports.

4. It is the responsibility of the TO Contractor to make sure that all subcontractors submit reports no later than the 15th of each month, regardless of whether there was any MBE payment activity for the reporting month. Actual payment data is verified and entered into the State's financial management tracking system from the subcontractor's D-6 report only. Therefore, if the subcontractor(s) do not submit their D-6 payment reports, the TO Contractor cannot and will not be given credit for subcontractor payments, regardless of the TO Contractor's proper submission of Form D-5. The TO Manager will contact the TO Contractor if reports are not received each month from either the prime contractor or any of

the identified subcontractors. The TO Contractor must promptly notify the TO Manager if, during the course of the contract, a new MBE subcontractor is utilized. Failure to comply with the MBE contract provisions and reporting requirements may result in sanctions, as provided by COMAR 21.11.03.13.

MDOT MBE FORM A
STATE-FUNDED CONTRACTS
CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT
PAGE 1 OF 2

This affidavit must be included with the bid/proposal. If the bidder/offeror fails to accurately complete and submit this affidavit as required, the bid shall be deemed not responsive or the proposal not susceptible of being selected for award.

In connection with the bid/proposal submitted in response to Solicitation No. , I affirm the following:

1. MBE Participation (PLEASE CHECK ONLY ONE)

☐ I have met the overall certified Minority Business Enterprise (MBE) participation goal of percent (%) and the following sub-goals, if applicable:
percent (%) for African American-owned MBE firms
percent (%) for Hispanic American-owned MBE firms
percent (%) for Asian American-owned MBE firms
percent (%) for Women-owned MBE firms
I agree that these percentages of the total dollar amount of the Contract, for the MBE goal and sub-goals (if any), will be performed by certified MBE firms as set forth in the MBE Participation Schedule - Part 2 of the MDOT MBE Form B (State-Funded Contracts).

OR

☐ I conclude that I am unable to achieve the MBE participation goal and/or sub-goals. I hereby request a waiver, in whole or in part, of the overall goal and/or sub-goals. Within 10 business days of receiving notice that our firm is the apparent awardee or as requested by the Procurement Officer, I will submit a written waiver request and all required documentation in accordance with COMAR 21.11.03.11. For a partial waiver request, I agree that certified MBE firms will be used to accomplish the percentages of the total dollar amount of the Contract, for the MBE goal and sub-goals (if any), as set forth in the MBE Participation Schedule - Part 2 of the MDOT MBE Form B (State-Funded Contracts).

2. Additional MBE Documentation

I understand that if I am notified that I am the apparent awardee or as requested by the Procurement Officer, I must submit the following documentation within 10 business days of receiving such notice:
(a) Outreach Efforts Compliance Statement (MDOT MBE Form C - State-Funded Contracts);
(b) Subcontractor Project Participation Statement (MDOT MBE Form D - State-Funded Contracts);
(c) If waiver requested, MBE Waiver Request Documentation and Forms (MDOT MBE/DBE Form E – Good Faith Efforts Guidance and Documentation) per COMAR 21.11.03.11; and

(d) Any other documentation required by the Procurement Officer to ascertain bidder's responsibility/ offeror's susceptibility of being selected for award in connection with the certified MBE participation goal and sub-goals, if any.

I acknowledge that if I fail to return each completed document (in 2 (a) through (d)) within the required time, the Procurement Officer may determine that I am not responsible and therefore not eligible for contract award or that the proposal is not susceptible of being selected for award.

MDOT MBE FORM A
STATE-FUNDED CONTRACTS
CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT
PAGE 2 OF 2

3. Information Provided to MBE firms

In the solicitation of subcontract quotations or offers, MBE firms were provided not less than the same information and amount of time to respond as were non-MBE firms.

4. Products and Services Provided by MBE firms

I hereby affirm that the MBEs are only providing those products and services for which they are MDOT certified.

I solemnly affirm under the penalties of perjury that the information in this affidavit is true to the best of my knowledge, information and belief.

_____	_____
Company Name	Signature of Representative
_____	_____
Address	Printed Name and Title
_____	_____
City, State and Zip Code	Date

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL. IF THE BIDDER/OFFEROR FAILS TO ACCURATELY COMPLETE AND SUBMIT PART 2 WITH THE BID/PROPOSAL AS REQUIRED, THE BID SHALL BE DEEMED NOT RESPONSIVE OR THE PROPOSAL SHALL BE DEEMED NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD.

PLEASE READ BEFORE COMPLETING THIS FORM

1. Please refer to the Maryland Department of Transportation (MDOT) MBE Directory at www.mdot.state.md.us to determine if a firm is certified for the appropriate North American Industry Classification System ("NAICS") Code **and** the product/services description (specific product that a firm is certified to provide or specific areas of work that a firm is certified to perform). For more general information about NAICS, please visit www.naics.com. Only those specific products and/or services for which a prime or subcontractor is a certified MBE in the MDOT Directory can be used for purposes of achieving the MBE participation goals.

2. In order to be counted for purposes of achieving the MBE participation goals, the MBE firm (whether a prime or subcontractor) must be certified for that specific NAICS Code ("MBE" for State-funded projects designation after NAICS Code). **WARNING:** If the firm's NAICS Code is in **graduated status**, such services/products **will not be counted** for purposes of achieving the MBE participation goals. Graduated status is clearly identified in the MDOT Directory (such graduated codes are designated with the word graduated after the appropriate NAICS Code).

3. Examining the NAICS Code is the **first step** in determining whether an MBE firm is certified and eligible to receive MBE participation credit for the specific products/services to be supplied or performed under the contract. The **second step** is to determine whether a firm's Products/Services Description in the MBE Directory includes the products to be supplied and/or services to be performed that are being used to achieve the MBE participation goals. If you have any questions as to whether a firm is certified to perform the specific services or provide specific products, please contact MDOT's Office of Minority Business Enterprise at 1-800-544-6056 or via email at mbe@mdot.state.md.us.

4. Complete the Part 2 – MBE Participation Schedule for all certified MBE firms (including primes and subcontractors) being used to achieve the MBE participation goal and sub-goals, if any.

5. **MBE Prime Self-Performance.** When a certified MBE firm participates as a prime (independently or as part of a joint venture) on a contract, a procurement agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own forces toward fulfilling up to fifty-percent (50%) of the MBE participation goal (overall) and up to one hundred percent (100%) of not more than one of the MBE participation sub-goals, if any, established for the contract. In order to receive credit for self-performance, an MBE prime must be (a) a certified MBE (see 1-3 above) and (b) listed in the Part 2 – MBE Participation Schedule with its certification number, the certification classification under which it will self-perform, and the percentage of the contract that can be counted as MBE self-performance. For the remaining portion of the overall goal and any sub-goals, the MBE prime must also list, in the Part 2 – MBE Participation Schedule, other certified MBE firms used to meet those goals or, after making good faith efforts to obtain the participation of additional MBE firms, request a waiver. Note: A dually-certified MBE firm can use its own forces toward fulfilling ONLY ONE of the MBE sub-goals for which it can be counted.

6. The Contractor's subcontractors are considered second-tier subcontractors. Third-tier contracting used to meet an MBE goal is to be considered the exception and not the rule. The following two conditions must be met before MDOT, its Modal Administrations and the Maryland Transportation Authority may approve a third-tier contracting agreement: (a) the bidder/offeror must request in writing approval of each third-tier contract arrangement, and (b) the request must contain specifics as to why a third-tier contracting arrangement should be approved. These documents must be submitted with the bid/proposal in Part 2 of this MBE Participation Schedule.

7. For each MBE firm that is being used as a supplier/wholesaler/regular dealer/broker/manufacturer, please follow these instructions for calculating the **amount of the subcontract for purposes of achieving the MBE participation goals**:

A. Is the firm certified as a broker of the products/supplies? If the answer is YES, please continue to Item C. If the answer is NO, please continue to Item B.

B. Is the firm certified as a supplier, wholesaler, regular dealer, or manufacturer of such products/supplies? If the answer is YES, continue to Item D. If the answer is NO, continue to Item C only if the MBE firm is certified to perform trucking/hauling services under NAICS Codes 484110, 484121, 484122, 484210, 484220 and 484230. If the answer is NO and the firm is not certified under these NAICS Codes, then no MBE participation credit will be given for the supply of these products.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

C. For purposes of achieving the MBE participation goal, you may count only the amount of any reasonable fee that the MBE firm will receive for the provision of such products/supplies - not the total subcontract amount or the value (or a percentage thereof) of such products and/or supplies. For Column 3 of the MBE Participation Schedule, please divide the amount of any reasonable fee that the MBE firm will receive for the provision of such products/services by the total Contract value and insert the percentage in Line 3.1.

D. Is the firm certified as a manufacturer (refer to the firm's NAICS Code and specific description of products/services) of the products/supplies to be provided? If the answer is NO, please continue to Item E. If the answer is YES, for purposes of achieving the MBE participation goal, you may count the total amount of the subcontract. For Column 3 of the MBE Participation Schedule, please divide the total amount of the subcontract by the total Contract value and insert the percentage in Line 3.1.

E. Is the firm certified as a supplier, wholesaler and/or regular dealer? If the answer is YES and the MBE firm is furnishing and installing the materials and is certified to perform these services, please divide the total subcontract amount (including full value of supplies) by the total Contract value and insert the percentage in Line 3.1. If the answer is YES and the MBE firm is only being used as a supplier, wholesaler and/or regular dealer or is not certified to install the supplies/materials, for purposes of achieving the MBE participation goal, you may only count sixty percent (60%) of the value of the subcontract for these supplies/products (60% Rule). To apply the 60% Rule, first divide the amount of the subcontract for these supplies/products only (not installation) by the total Contract value. Then, multiply the result by sixty percent (60%) and insert the percentage in Line 3.2.

8. For each MBE firm that **is not** being used as a supplier/wholesaler/regular dealer/broker/manufacturer, to calculate the **amount of the subcontract for purposes of achieving the MBE participation goals**, divide the total amount of the subcontract by the total Contract value and insert the percentage in Line 3.1.

Example: $ 2,500 (Total Subcontract Amount) ÷ $10,000 (Total Contract Value) x 100 = 25%

9. **WARNING:** The percentage of MBE participation, computed using the percentage amounts determined per Column 3 for all of the MBE firms listed in Part 2, MUST at least equal the MBE participation goal **and** sub-goals (if applicable) as set forth in MDOT MBE Form A – State-Funded Contracts for this solicitation. If a bidder/offeror is unable to achieve the MBE participation goal and/or any sub-goals (if applicable), then the bidder/offeror must request a waiver in Form A or the bid will be deemed not responsive, or the proposal not susceptible of being selected for award. You may wish to use the attached Goal/Sub-goal Worksheet to assist you in calculating the percentages and confirming that you have met the applicable MBE participation goal and sub-goals (if any).

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 1 – INSTRUCTIONS FOR MBE PARTICIPATION SCHEDULE

GOAL/SUBGOAL PARTICIPATION WORKSHEET

1. Complete the Part 2 – MBE Participation Schedule for each MBE being used to meet the MBE goal and any sub-goals.

2. After completion of the Part 2 – MBE Participation Schedule, you may use the Goal/Sub-goal Worksheet to calculate the total MBE participation commitment for the overall goal and any sub-goals.

3. **MBE Overall Goal Participation Boxes:** Calculate the total percentage of MBE participation for each MBE classification by adding the percentages determined per Column 3 of the Part 2 – MBE Participation Schedule. Add the percentages determined in Lines 3.1 and 3.2 for the MBE subcontractor (subs) total. Add the overall participation percentages determined in Line 3.3 for the MBE prime total.

4. **MBE Subgoal Participation Boxes:** Calculate the total percentage of MBE participation for each MBE classification by adding the percentages determined per Column 3 of the Part 2 – MBE Participation Schedule. Add the percentages determined in Lines 3.1 and 3.2 for the MBE subcontractor (subs) total. Add the subgoal participation percentages determined in Line 3.3 for the MBE prime total.

5. The percentage amount for the MBE overall participation in the Total MBE Firm Participation Box F1 should be equal to the sum of the percentage amounts in Boxes A through E of the MBE Overall Goal Participation Column of the Worksheet.

6. The percentage amount for the MBE subgoal participation in the Total MBE Firm Participation Box L should be equal to the sum of the percentage amounts in Boxes A through E of the MBE Subgoal Participation Column of the Worksheet.

GOAL/SUBGOAL WORKSHEET		
MBE Classification	**MBE Overall Goal Participation**	**MBE Subgoal Participation**
(A) Total African American Firm Participation (Add percentages determined for African American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(B) Total Hispanic American Firm Participation (Add percentages determined for Hispanic American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(C) Total Asian American Firm Participation (Add percentages listed for Asian American-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(D) Total Women-Owned Firm Participation (Add percentages determined for Women-Owned Firms per Column 3 of MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
(E) Total for all other MBE Firms (Add percentages for firms listed as Other MBE Classification per Column 3 of the MBE Participation Schedule)	_____%subs _____%prime	_____%subs _____%prime
Total MBE Firm Participation (Add total percentages determined for all MBE Firms in each column of the Worksheet)	**(F1)**_____%	**(F2)**_____%

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 2 – MBE PARTICIPATION SCHEDULE

PAGE __ OF ___

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL. IF THE BIDDER/OFFEROR FAILS TO ACCURATELY COMPLETE AND SUBMIT PART 2 WITH THE BID/PROPOSAL AS REQUIRED, THE BID SHALL BE DEEMED NOT RESPONSIVE OR THE PROPOSAL SHALL BE DEEMED NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD.

Prime Contractor	Project Description	SOLICITATION NUMBER

LIST INFORMATION FOR EACH CERTIFIED MBE PRIME OR MBE SUBCONTRACTOR YOU AGREE TO USE TO ACHIEVE THE MBE PARTICIPATION GOAL AND SUB-GOALS, IF ANY. NOTE INSTRUCTIONS IN EACH COLUMN.

COLUMN 1	**COLUMN 2**	**COLUMN 3** Unless the bidder/offeror requested a waiver in MDOT MBE Form A – State Funded Contracts for this solicitation, the cumulative MBE participation for all MBE firms listed herein must equal at least the MBE participation goal and sub-goals (if applicable) set forth in Form A.
NAME OF MBE PRIME OR MBE SUBCONTRACTOR AND TIER	**CERTIFICATION NO. AND MBE CLASSIFICATION**	FOR PURPOSES OF ACHIEVING THE MBE PARTICIPATION GOAL AND SUB-GOALS, refer to Sections 5 through 8 in Part 1 - Instructions. State the percentage amount of the products/services in Line 3.1, except for those products or services where the MBE firm is being used as a wholesaler, supplier, or regular dealer. For items of work where the MBE firm is being used as a supplier, wholesaler and/or regular dealer, complete Line 3.2 using the 60% Rule. For items of work where the MBE firm is the prime, complete Line 3.3.
MBE Name: _____ ☐ Check here if MBE firm is a subcontractor and complete in accordance with Sections 6, 7, & 8 of Part 1 - Instructions. If this box is checked, complete 3.1 or 3.2 in Column C, whichever is appropriate. ☐ Check here if MBE firm is the prime contractor, including a participant in a joint venture, and self-performance is being counted pursuant to Section 5 of Part 1 - Instructions. If this box is checked, complete 3.3 in Column C. ☐ Check here if MBE firm is a third-tier contractor (if applicable). Please submit written documents in	**Certification Number:** _____ **(If dually certified, check only one box.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____	3.1. **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE- EXCLUDING PRODUCTS/SERVICES FROM SUPPLIERS, WHOLESALERS OR REGULAR DEALERS). **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.2 **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR FOR ITEMS OF WORK WHERE THE MBE FIRM IS BEING USED AS A SUPPLIER, WHOLESALER AND/OR REGULAR DEALER)** (STATE THE PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE AND THEN APPLY THE 60% RULE PER SECTION 7(E) IN PART 1 - INSTRUCTIONS). _____% Total percentage of Supplies/Products **x _____ 60% (60% Rule)** **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.3. **TOTAL PERCENTAGE TO BE PAID TO MBE PRIME FOR WORK THAT CAN BE COUNTED AS MBE SELF-PERFORMANCE** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE).

accordance with Section 6 of Part 1 - Instructions		**(a) _____ % Total percentage for self-performed items of work in which MBE is certified)** **(b) _____ % (Insert 50% of MBE overall goal)** **(c) _____ % (Insert subgoal for classification checked in Column 2, if applicable)** **Percentages for purposes of calculating achievement of MBE Participation goals:** **➡ For MBE Overall goal – Use lesser of (a) or (b)** **➡ For MBE Subgoal – Use lesser of (a) or (c)** **➡ If MBE Prime is supplier, wholesaler and/or regular dealer, apply the 60% rule.**

☐Check here if Continuation Sheets are attached.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 2 – MBE PARTICIPATION SCHEDULE
CONTINUATION SHEET

PAGE __ OF ___

Prime Contractor	Project Description	1. SOLICITATION NUMBER

LIST INFORMATION FOR EACH CERTIFIED MBE PRIME OR MBE SUBCONTRACTOR YOU AGREE TO USE TO ACHIEVE THE MBE PARTICIPATION GOAL AND SUB-GOALS, IF ANY. NOTE INSTRUCTIONS IN EACH COLUMN.

COLUMN 1	COLUMN 2	COLUMN 3 Unless the bidder/offeror requested a waiver in MDOT MBE Form A – State Funded Contracts for this solicitation, the cumulative MBE participation for all MBE firms listed herein must equal at least the MBE participation goal and sub-goals (if applicable) set forth in Form A.
NAME OF MBE PRIME OR MBE SUBCONTRACTOR AND TIER	**CERTIFICATION NO. AND MBE CLASSIFICATION**	FOR PURPOSES OF ACHIEVING THE MBE PARTICIPATION GOAL AND SUB-GOALS, refer to Sections 5 through 8 in Part 1 - Instructions. State the percentage amount of the products/services in Line 3.1, except for those products or services where the MBE firm is being used as a wholesaler, supplier, or regular dealer. For items of work where the MBE firm is being used as a supplier, wholesaler and/or regular dealer, complete Line 3.2 using the 60% Rule. For items of work where the MBE firm is the prime, complete Line 3.3.
MBE Name: _____ ☐ Check here if MBE firm is a subcontractor and complete in accordance with Sections 6, 7, & 8 of Part 1 - Instructions. If this box is checked, complete 3.1 or 3.2 in Column C, whichever is appropriate. ☐ Check here if MBE firm is the prime contractor, including a participant in a joint venture, and self-performance is being counted pursuant to Section 5 of Part 1 - Instructions. If this box is checked, complete 3.3 in Column C. ☐ Check here if MBE firm is a third-tier contractor (if applicable). Please submit written documents in	**Certification Number:** _____ **(If dually certified, check only one box.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____	3.1. **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE- EXCLUDING PRODUCTS/SERVICES FROM SUPPLIERS, WHOLESALERS OR REGULAR DEALERS). **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.2 **TOTAL PERCENTAGE TO BE PAID TO THE SUBCONTRACTOR FOR ITEMS OF WORK WHERE THE MBE FIRM IS BEING USED AS A SUPPLIER, WHOLESALER AND/OR REGULAR DEALER)** (STATE THE PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE AND THEN APPLY THE 60% RULE PER SECTION 7(E) IN PART 1 - INSTRUCTIONS). _____% Total percentage of Supplies/Products **x _____60% (60% Rule)** **_____% (Percentage for purposes of calculating achievement of MBE Participation goal and sub-goals, if any)** 3.3. **TOTAL PERCENTAGE TO BE PAID TO MBE PRIME FOR WORK THAT CAN BE COUNTED AS MBE SELF-PERFORMANCE** (STATE THIS PERCENTAGE AS A PERCENTAGE OF THE TOTAL CONTRACT VALUE)..

accordance with Section 6 of Part 1 - Instructions		**(a) _____ % Total percentage for self-performed items of work in which MBE is certified)** **(b) _____ % (Insert 50% of MBE overall goal)** **(c) _____ % (Insert subgoal for classification checked in Column 2, if applicable)** **Percentages for purposes of calculating achievement of MBE Participation goals:** **➡ For MBE Overall goal – Use lesser of (a) or (b)** **➡ For MBE Subgoal – Use lesser of (a) or (c)** **➡If MBE Prime is supplier, wholesaler and/or regular dealer, apply the 60% rule.**

☐Check here if Continuation Sheets are attached.

MDOT MBE FORM B
STATE-FUNDED CONTRACTS
PART 3 – CERTIFICATION FOR MBE PARTICIPATION SCHEDULE

PARTS 2 AND 3 MUST BE INCLUDED WITH THE BID/PROPOSAL AS DIRECTED IN THE INVITATION TO BID/ REQUEST FOR PROPOSALS.

I hereby affirm that I have reviewed the Products and Services Description (specific product that a firm is certified to provide or areas of work that a firm is certified to perform) set forth in the MDOT MBE Directory for each of the MBE firms listed in Part 2 of this MBE Form B for purposes of achieving the MBE participation goals and sub-goals that were identified in the MBE Form A that I submitted with this solicitation, and that the MBE firms listed are only performing those products/services/areas of work for which they are certified. I also hereby affirm that I have read and understand the form instructions set forth in Part 1 of this MBE Form B.

The undersigned Prime Contractor hereby certifies and agrees that they have fully complied with the State Minority Business Enterprise law, State Finance and Procurement Article §14-308(a)(2), Annotated Code of Maryland which provides that, except as otherwise provided by law, a contractor may not identify a certified minority business enterprise in a bid or proposal and:

(1) fail to request, receive, or otherwise obtain authorization from the certified minority business enterprise to identify the certified minority business enterprise in its bid or proposal;

(2) fail to notify the certified minority business enterprise before execution of the contract of its inclusion of the bid or proposal;

(3) fail to use the certified minority business enterprise in the performance of the contract; or

(4) pay the certified minority business enterprise solely for the use of its name in the bid or proposal.

I solemnly affirm under the penalties of perjury that the contents of Parts 2 and 3 of MDOT MBE Form B are true to the best of my knowledge, information and belief.

Company Name	Signature of Representative
Address	Printed Name and Title
City, State and Zip Code	Date

MDOT MBE FORM C
STATE-FUNDED CONTRACTS
OUTREACH EFFORTS COMPLIANCE STATEMENT

In conjunction with the offer/proposal submitted in response to Solicitation No._____, I state the following:

1. Bidder/Offeror took the following efforts to identify subcontracting opportunities in these specific work categories:

2. Attached to this form are copies of written solicitations (with bidding/proposal instructions) used to solicit certified MBE firms for these subcontract opportunities.

3. Bidder/Offeror made the following attempts to personally contact the solicited MBE firms:

4. **Please Check One:**

☐ This project does not involve bonding requirements.

☐ Bidder/Offeror assisted MBE firms to fulfill or seek waiver of bonding requirements. (DESCRIBE EFFORTS)

5. **Please Check One:**

☐ Bidder/Offeror did attend the pre-bid/pre-proposal meeting/conference.

☐ No pre-bid/pre-proposal meeting/conference was held.

☐ Bidder/Offeror did not attend the pre-bid/pre-proposal meeting/conference.

_____	_____
Company Name	Signature of Representative
_____	_____
Address	Printed Name and Title
_____	_____
City, State and Zip Code	Date

MDOT MBE FORM D
STATE-FUNDED CONTRACTS
MBE SUBCONTRACTOR PROJECT PARTICIPATION AFFIDAVIT

IF THE BIDDER/OFFEROR FAILS TO RETURN THIS AFFIDAVIT WITHIN THE REQUIRED TIME, THE PROCUREMENT OFFICER MAY DETERMINE THAT THE BIDDER/OFFEROR IS NOT RESPONSIBLE AND THEREFORE NOT ELIGIBLE FOR CONTRACT AWARD OR THAT THE PROPOSAL IS NOT SUSCEPTIBLE OF BEING SELECTED FOR AWARD. SUBMIT ONE FORM FOR EACH CERTIFIED MBE FIRM LISTED IN THE MBE PARTICIPATION SCHEDULE. BIDDERS/OFFERORS ARE HIGHLY ENCOURAGED TO SUBMIT FORM D PRIOR TO THE TEN (10) DAY DEADLINE.

Provided that _____ (Prime Contractor's Name) is awarded the State contract in conjunction with Solicitation No. _____, such Prime Contractor will enter into a subcontract with _____(Subcontractor's Name) committing to participation by the MBE firm _____ (MBE Name) with MDOT Certification Number _____ (if subcontractor previously listed is also the MBE firm, please restate name and provide MBE Certification Number) which will receive at least $_____ or ___% (Total Subcontract Amount/ Percentage) for performing the following products/services for the Contract:

NAICS CODE	WORK ITEM, SPECIFICATION NUMBER, LINE ITEMS OR WORK CATEGORIES (IF APPLICABLE)	DESCRIPTION OF SPECIFIC PRODUCTS AND/OR SERVICES

I solemnly affirm under the penalties of perjury that the information provided in this MBE Subcontractor Project Participation Affidavit is true to the best of my knowledge, information and belief. I acknowledge that, for purposes of determining the accuracy of the information provided herein, the Procurement Officer may request additional information, including, without limitation, copies of the subcontract agreements and quotes.

PRIME CONTRACTOR	SUBCONTRACTOR (SECOND-TIER)	SUBCONTRACTOR (THIRD-TIER)
Signature of Representative: _____ __ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____ _____ ___	Signature of Representative: _____ ___ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____	Signature of Representative: _____ ___ Printed Name and Title:_____ _____ ___ Firm's Name: _____ Federal Identification Number: _____ Address: _____

Telephone: _____ Date: _____	_____ Telephone: _____ Date: _____	_____ Telephone: _____ Date: _____

IF MBE FIRM IS A THIRD-TIER SUBCONTRACTOR, THIS FORM MUST ALSO BE EXECUTED BY THE SECOND-TIER SUBCONTRACTOR THAT HAS THE SUBCONTRACT AGREEMENT WITH THE MBE FIRM.

This form is to be completed monthly by the prime contractor.

Attachment D-5

Maryland Department of Information Technology
Minority Business Enterprise Participation
Prime Contractor Paid/Unpaid MBE Invoice Report

Report #: _____ Reporting Period (Month/Year): _____ **Report is due to the MBE Officer by the 10th of the month following the month the services were provided.** **Note: Please number reports in sequence**	Contract #: _____ Contracting Unit: _____ Contract Amount: _____ MBE Subcontract Amt: _____ Project Begin Date: _____ Project End Date: _____ Services Provided: _____

Prime Contractor:	Contact Person:	
Address:		
City:	State:	ZIP:
Phone:	FAX:	Email:
Subcontractor Name:	Contact Person:	
Phone:	FAX:	
Subcontractor Services Provided:		

List all payments made to MBE subcontractor named above during this reporting period: **Invoice# Amount** **1.** **2.** **3.** **4.** **Total Dollars Paid: $**_____	**List dates and amounts of any outstanding invoices:** **Invoice # Amount** **1.** **2.** **3.** **4.** **Total Dollars Unpaid:** **$**_____

**If more than one MBE subcontractor is used for this contract, you must use separate D-5 forms.

****Return one copy (hard or electronic) of this form to the following addresses (electronic copy with signature and date is preferred):**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)

This form must be completed by MBE subcontractor

ATTACHMENT D-6
Minority Business Enterprise Participation
Subcontractor Paid/Unpaid MBE Invoice Report

Report#: ____ Reporting Period (Month/Year): _____ **Report is due by the 10th of the month following the month the services were performed.**	Contract # Contracting Unit: MBE Subcontract Amount: Project Begin Date: Project End Date: Services Provided:

MBE Subcontractor Name:		
MDOT Certification #:		
Contact Person:	Email:	
Address:		
City: Baltimore	State:	ZIP:
Phone:	FAX:	

Subcontractor Services Provided:

List all payments received from Prime Contractor during reporting period indicated above.	**List dates and amounts of any unpaid invoices over 30 days old.**
Invoice Amt **Date** **1.** **2.** **3.** **Total Dollars Paid: $**_____	**Invoice Amt** **Date** **1.** **2.** **3.** **Total Dollars Unpaid:** **$**_____

Prime Contractor: Contact Person:

****Return one copy of this form to the following address (electronic copy with signature & date is preferred):**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)

Signature: _____ Date: _____
(Required)

ATTACHMENT 2 - MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 1 – Guidance for Demonstrating Good Faith Efforts to Meet MBE/DBE Participation Goals

In order to show that it has made good faith efforts to meet the Minority Business Enterprise (MBE)/Disadvantaged Business Enterprise (DBE) participation goal (including any MBE sub-goals) on a contract, the bidder/offeror must either (1) meet the MBE/DBE Goal(s) and document its commitments for participation of MBE/DBE Firms, or (2) when it does not meet the MBE/DBE Goal(s), document its Good Faith Efforts to meet the goal(s).

I. Definitions

MBE/DBE Goal(s) – "MBE/DBE Goal(s)" refers to the MBE participation goal and MBE participation sub-goal(s) on a State-funded procurement and the DBE participation goal on a federally-funded procurement.

Good Faith Efforts – The "Good Faith Efforts" requirement means that when requesting a waiver, the bidder/offeror must demonstrate that it took all necessary and reasonable steps to achieve the MBE/DBE Goal(s), which, by their scope, intensity, and appropriateness to the objective, could reasonably be expected to obtain sufficient MBE/DBE participation, even if those steps were not fully successful. Whether a bidder/offeror that requests a waiver made adequate good faith efforts will be determined by considering the quality, quantity, and intensity of the different kinds of efforts that the bidder/offeror has made. The efforts employed by the bidder/offeror should be those that one could reasonably expect a bidder/offeror to take if the bidder/offeror were actively and aggressively trying to obtain DBE participation sufficient to meet the DBE contract goal. Mere *pro forma* efforts are not good faith efforts to meet the DBE contract requirements. The determination concerning the sufficiency of the bidder's/offeror's good faith efforts is a judgment call; meeting quantitative formulas is not required.

Identified Firms – "Identified Firms" means a list of the DBEs identified by the procuring agency during the goal setting process and listed in the federally-funded procurement as available to perform the Identified Items of Work. It also may include additional DBEs identified by the bidder/offeror as available to perform the Identified Items of Work, such as DBEs certified or granted an expansion of services after the procurement was issued. If the procurement does not include a list of Identified Firms or is a State-funded procurement, this term refers to all of the MBE Firms (if State-funded) or DBE Firms (if federally-funded) the bidder/offeror identified as available to perform the Identified Items of Work and should include all appropriately certified firms that are reasonably identifiable.

Identified Items of Work – "Identified Items of Work" means the bid items identified by the procuring agency during the goal setting process and listed in the procurement as possible items of work for performance by MBE/DBE Firms. It also may include additional portions of items of work the bidder/offeror identified for performance by MBE/DBE Firms to increase the likelihood that the MBE/DBE Goal(s) will be achieved. If the procurement does not include a list of Identified Items of Work, this term refers to all of the items of work the bidder/offeror identified as possible items of work for performance by MBE/DBE Firms and should include all reasonably identifiable work opportunities.

MBE/DBE Firms – For State-funded contracts, "MBE/DBE Firms" refers to certified **MBE** Firms. Certified MBE Firms can participate in the State's MBE Program. For federally-funded contracts, "MBE/DBE Firms" refers to certified **DBE** Firms. Certified DBE Firms can participate in the federal DBE Program.

II. Types of Actions MDOT will Consider

The bidder/offeror is responsible for making relevant portions of the work available to MBE/DBE subcontractors and suppliers and to select those portions of the work or material needs consistent with the available MBE/DBE subcontractors and suppliers, so as to facilitate MBE/DBE participation. The following is a list of types of actions MDOT will consider as part of the bidder's/offeror's Good Faith Efforts when the bidder/offeror fails to meet the

MBE/DBE Goal(s). This list is not intended to be a mandatory checklist, nor is it intended to be exclusive or exhaustive. Other factors or types of efforts may be relevant in appropriate cases.

A. Identify Bid Items as Work for MBE/DBE Firms

1. Identified Items of Work in Procurements

(a) Certain procurements will include a list of bid items identified during the goal setting process as possible work for performance by MBE/DBE Firms. If the procurement provides a list of Identified Items of Work, the bidder/offeror shall make all reasonable efforts to solicit quotes from MBE Firms or DBE Firms, whichever is appropriate, to perform that work.

(b) Bidders/Offerors may, and are encouraged to, select additional items of work to be performed by MBE/DBE Firms to increase the likelihood that the MBEDBE Goal(s) will be achieved.

2. Identified Items of Work by Bidders/Offerors

(a) When the procurement does not include a list of Identified Items of Work, bidders/offerors should reasonably identify sufficient items of work to be performed by MBE/DBE Firms.

(b) Where appropriate, bidders/offerors should break out contract work items into economically feasible units to facilitate MBE/DBE participation, rather than perform these work items with their own forces. The ability or desire of a prime contractor to perform the work of a contract with its own organization does not relieve the bidder/offeror of the responsibility to make Good Faith Efforts.

B. Identify MBE Firms or DBE Firms to Solicit

1. DBE Firms Identified in Procurements

(a) Certain procurements will include a list of the DBE Firms identified during the goal setting process as available to perform the items of work. If the procurement provides a list of Identified DBE Firms, the bidder/offeror shall make all reasonable efforts to solicit those DBE firms.

(b) Bidders/offerors may, and are encouraged to, search the MBE/DBE Directory to identify additional DBEs who may be available to perform the items of work, such as DBEs certified or granted an expansion of services after the solicitation was issued.

2. MBE/DBE Firms Identified by Bidders/Offerors

(a) When the procurement does not include a list of Identified MBE/DBE Firms, bidders/offerors should reasonably identify the MBE Firms or DBE Firms, whichever is appropriate, that are available to perform the Identified Items of Work.

(b) Any MBE/DBE Firms identified as available by the bidder/offeror should be certified in the appropriate program (MBE for State-funded procurements or DBE for federally-funded procurements)

(c) Any MBE/DBE Firms identified as available by the bidder/offeror should be certified to perform the Identified Items of Work.

C. Solicit MBE/DBEs

1. Solicit <u>all</u> Identified Firms for all Identified Items of Work by providing written notice. The bidder/offeror should:

(a) provide the written solicitation at least 10 days prior to bid opening to allow sufficient time for the MBE/DBE Firms to respond;

(b) send the written solicitation by first-class mail, facsimile, or email using contact information in the MBE/DBE Directory, unless the bidder/offeror has a valid basis for using different contact information; and

(c) provide adequate information about the plans, specifications, anticipated time schedule for portions of the work to be performed by the MBE/DBE, and other requirements of the contract to assist MBE/DBE Firms in responding. (This information may be provided by including hard copies in the written solicitation or by electronic means as described in C.3 below.)

2. "All" Identified Firms includes the DBEs listed in the procurement and any MBE/DBE Firms you identify as potentially available to perform the Identified Items of Work, but it does not include MBE/DBE Firms who are no longer certified to perform the work as of the date the bidder/offeror provides written solicitations.

3. "Electronic Means" includes, for example, information provided *via* a website or file transfer protocol (FTP) site containing the plans, specifications, and other requirements of the contract. If an interested MBE/DBE cannot access the information provided by electronic means, the bidder/offeror must make the information available in a manner that is accessible by the interested MBE/DBE.

4. Follow up on initial written solicitations by contacting DBEs to determine if they are interested. The follow up contact may be made:

(a) by telephone using the contact information in the MBE/DBE Directory, unless the bidder/offeror has a valid basis for using different contact information; or

(b) in writing *via* a method that differs from the method used for the initial written solicitation.

5. In addition to the written solicitation set forth in C.1 and the follow up required in C.4, use all other reasonable and available means to solicit the interest of MBE/DBE Firms certified to perform the work of the contract. Examples of other means include:

(a) attending any pre-bid meetings at which MBE/DBE Firms could be informed of contracting and subcontracting opportunities;

(b) if recommended by the procurement, advertising with or effectively using the services of at least two minority focused entities or media, including trade associations, minority/women community organizations, minority/women contractors' groups, and local, state, and federal minority/women business assistance offices listed on the MDOT Office of Minority Business Enterprise website; and

(c) effectively using the services of other organizations, as allowed on a case-by-case basis and authorized in the procurement, to provide assistance in the recruitment and placement of MBE/DBE Firms.

D. Negotiate With Interested MBE/DBE Firms

Bidders/Offerors must negotiate in good faith with interested MBE/DBE Firms.

1. Evidence of negotiation includes, without limitation, the following:

(a) the names, addresses, and telephone numbers of MBE/DBE Firms that were considered;

(b) a description of the information provided regarding the plans and specifications for the work selected for subcontracting and the means used to provide that information; and

(c) evidence as to why additional agreements could not be reached for MBE/DBE Firms to perform the work.

2. A bidder/offeror using good business judgment would consider a number of factors in negotiating with subcontractors, including DBE subcontractors, and would take a firm's price and capabilities as well as contract goals into consideration.

3. The fact that there may be some additional costs involved in finding and using MBE/DBE Firms is not in itself sufficient reason for a bidder's/offeror's failure to meet the contract DBE goal, as long as such costs are reasonable. Factors to take into consideration when determining whether a MBE/DBE Firm's quote is excessive or unreasonable include, without limitation, the following:

(a) the dollar difference between the MBE/DBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(b) the percentage difference between the MBE/DBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(c) the percentage that the DBE subcontractor's quote represents of the overall contract amount;

(d) the number of MBE/DBE firms that the bidder/offeror solicited for that portion of the work;

(e) whether the work described in the MBE/DBE and Non-MBE/DBE subcontractor quotes (or portions thereof) submitted for review is the same or comparable; and

(f) the number of quotes received by the bidder/offeror for that portion of the work.

4. The above factors are not intended to be mandatory, exclusive, or exhaustive, and other evidence of an excessive or unreasonable price may be relevant.

5. The bidder/offeror may not use its price for self-performing work as a basis for rejecting a MBE/DBE Firm's quote as excessive or unreasonable.

6. The "average of the other subcontractors' quotes received by the" bidder/offeror refers to the average of the quotes received from all subcontractors, except that there should be quotes from at least three subcontractors, and there must be at least one quote from a MBE/DBE and one quote from a Non-MBE/DBE.

7. A bidder/offeror shall not reject a MBE/DBE Firm as unqualified without sound reasons based on a thorough investigation of the firm's capabilities. For each certified MBE/DBE that is rejected as unqualified or that placed a subcontract quotation or offer that the bidder/offeror concludes is not acceptable, the bidder/offeror must provide a written detailed statement listing the reasons for this conclusion. The bidder/offeror also must document the steps taken to verify the capabilities of the MBE/DBE and Non-MBE/DBE Firms quoting similar work.

(a) The factors to take into consideration when assessing the capabilities of a MBE/DBE Firm, include, but are not limited to the following: financial capability, physical capacity to perform, available personnel and equipment, existing workload, experience performing the type of work, conduct and performance in previous contracts, and ability to meet reasonable contract requirements.

(b) The MBE/DBE Firm's standing within its industry, membership in specific groups, organizations, or associations and political or social affiliations (for example union vs. non-union employee status) are not legitimate causes for the rejection or non-solicitation of bids in the efforts to meet the project goal.

E. Assisting Interested MBE/DBE Firms

When appropriate under the circumstances, the decision-maker will consider whether the bidder/offeror:

1. made reasonable efforts to assist interested MBE/DBE Firms in obtaining the bonding, lines of credit, or insurance required by MDOT or the bidder/offeror; and

2. made reasonable efforts to assist interested MBE/DBE Firms in obtaining necessary equipment, supplies, materials, or related assistance or services.

III. Other Considerations

In making a determination of Good Faith Efforts the decision-maker may consider engineering estimates, catalogue prices, general market availability and availability of certified MBE/DBE Firms in the area in which the work is to be performed, other bids or offers and subcontract bids or offers substantiating significant variances between certified MBE/DBE and Non-MBE/DBE costs of participation, and their impact on the overall cost of the contract to the State and any other relevant factors.

The decision-maker may take into account whether a bidder/offeror decided to self-perform subcontract work with its own forces, especially where the self-performed work is Identified Items of Work in the procurement. The decision-maker also may take into account the performance of other bidders/offerors in meeting the contract. For example, when the apparent successful bidder/offeror fails to meet the contract goal, but others meet it, this reasonably raises the question of whether, with additional reasonable efforts, the apparent successful bidder/offeror could have met the goal. If the apparent successful bidder/offeror fails to meet the goal, but meets or exceeds the average MBE/DBE participation obtained by other bidders/offerors, this, when viewed in conjunction with other factors, could be evidence of the apparent successful bidder/offeror having made Good Faith Efforts.

IV. Documenting Good Faith Efforts

At a minimum, a bidder/offeror seeking a waiver of the MBE/DBE Goal(s) or a portion thereof must provide written documentation of its Good Faith Efforts, in accordance with COMAR 21.11.03.11, within 10 business days after receiving notice that it is the apparent awardee. The written documentation shall include the following:

A. Items of Work (Complete Good Faith Efforts Documentation Form E, Part 2)

A detailed statement of the efforts made to select portions of the work proposed to be performed by certified MBE/DBE Firms in order to increase the likelihood of achieving the stated MBE/DBE Goal(s).

B. Outreach/Solicitation/Negotiation

1. The record of the bidder's/offeror's compliance with the outreach efforts prescribed by COMAR 21.11.03.09C (2)(a) through (e) and 49 C.F.R. Part 26, Appendix A. **(Complete Outreach Efforts Compliance Statement)**

2. A detailed statement of the efforts made to contact and negotiate with MBE/DBE Firms including:

(a) the names, addresses, and telephone numbers of the MBE/DBE Firms who were contacted, with the dates and manner of contacts (letter, fax, email, telephone, etc.) **(Complete Good Faith Efforts Form E, Part 3, and submit letters, fax cover sheets, emails, etc. documenting solicitations)**; and

(b) a description of the information provided to MBE/DBE Firms regarding the plans, specifications, and anticipated time schedule for portions of the work to be performed and the means used to provide that information.

C. Rejected MBE/DBE Firms (Complete Good Faith Efforts Form E, Part 4)

1. For each MBE/DBE Firm that the bidder/offeror concludes is not acceptable or qualified, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the steps taken to verify the capabilities of the MBE/DBE and Non-MBE/DBE Firms quoting similar work.

2. For each certified MBE/DBE Firm that the bidder/offeror concludes has provided an excessive or unreasonable price, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the quotes received from all MBE/DBE and Non-MBE/DBE firms bidding on the same or comparable work. **(Include copies of all quotes received.)**

3. A list of MBE/DBE Firms contacted but found to be unavailable. This list should be accompanied by a Minority Contractor Unavailability Certificate signed by the MBE/DBE contractor or a statement from the bidder/offeror that the MBE/DBE contractor refused to sign the Minority Contractor Unavailability Certificate.

D. Other Documentation

1. Submit any other documentation requested by the Procurement Officer to ascertain the bidder's/offeror's Good Faith Efforts.

2. Submit any other documentation the bidder/offeror believes will help the Procurement Officer ascertain its Good Faith Efforts.

ATTACHMENT 2 - MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 2 – Certification Regarding Goof Faith Efforts and Documentation

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

PARTS 3, 4, AND 5 MUST BE INCLUDED WITH THIS CERTIFICATE ALONG WITH ALL DOCUMENTS SUPPORTING YOUR WAIVER REQUEST.

I hereby request a waiver of (1) the Minority Business Enterprise (MBE) participation goal and/or subgoal(s), (2) the Disadvantaged Business Enterprise (DBE) participation goal, or (3) a portion of the pertinent MBE/DBE participation goal and/or MBE subgoal(s) for this procurement.[1] I affirm that I have reviewed the Good Faith Efforts Guidance MBE/DBE Form E. I further affirm under penalties of perjury that the contents of Parts 3, 4, and 5 of MDOT MBE/DBE Form E are true to the best of my knowledge, information and belief.

Company Name — Signature of Representative

Address — Printed Name and Title

City, State and Zip Code — Date

[1] MBE participation goals and sub-goals apply to State-funded procurements. DBE participation goals apply to federally-funded procurements. Federally-funded contracts do not have sub-goals.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 3 – Identified Items of Work Bidder/Offeror Made Available to MBE/dBE Firms

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

Identify those items of work that the bidder/offeror made available to MBE/DBE Firms. This includes, where appropriate, those items the bidder/offeror identified and determined to subdivide into economically feasible units to facilitate the MBE/DBE participation. For each item listed, show the anticipated percentage of the total contract amount. It is the bidder's/offeror's responsibility to demonstrate that sufficient work to meet the goal was made available to MBE/DBE Firms, and the total percentage of the items of work identified for MBE/DBE participation equals or exceeds the percentage MBE/DBE goal set for the procurement. Note: If the procurement includes a list of bid items identified during the goal setting process as possible items of work for performance by MBE/DBE Firms, the bidder/offeror should make all of those items of work available to MBE/DBE Firms or explain why that item was not made available. If the bidder/offeror selects additional items of work to make available to MBE/DBE Firms, those additional items should also be included below.

Identified Items of Work	Was this work listed in the procurement?	Does bidder/offeror normally self-perform this work?	Was this work made available to MBE/DBE Firms? If no, explain why?
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No

	□ Yes □ No	□ Yes □ No	□ Yes □ No

☐Please check if Additional Sheets are attached.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 4 – Identified MBE/DBE Firms and Record of Solicitations

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

Identify the MBE/DBE Firms solicited to provide quotes for the Identified Items of Work made available for MBE/DBE participation. Include the name of the MBE/DBE Firm solicited, items of work for which bids/quotes were solicited, date and manner of initial and follow-up solicitations, whether the MBE/DBE provided a quote, and whether the MBE/DBE is being used to meet the MBE/DBE participation goal. MBE/DBE Firms used to meet the participation goal must be included on the MBE/DBE Participation Schedule, Form B. Note: If the procurement includes a list of the MBE/DBE Firms identified during the goal setting process as potentially available to perform the items of work, the bidder/offeror should solicit all of those MBE/DBE Firms or explain why a specific MBE/DBE was not solicited. If the bidder/offeror identifies additional MBE/DBE Firms who may be available to perform Identified Items of Work, those additional MBE/DBE Firms should also be included below. Copies of all written solicitations and documentation of follow-up calls to MBE/DBE Firms must be attached to this form. If the bidder/offeror used a Non-MBE/DBE or is self-performing the identified items of work, Part 4 must be completed.

Name of Identified MBE/DBE Firm & MBE Classification	Describe Item of Work Solicited	Initial Solicitation Date & Method	Follow-up Solicitation Date & Method	Details for Follow-up Calls	Quote Rec'd	Quote Used	Reason Quote Rejected
Firm Name: _____ **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification _____		Date: □ Mail □ Facsimile □ Email	Date: □ Phone □ Mail □ Facsimile □ Email	Time of Call: Spoke With: □ Left Message	□ Yes □ No	□ Yes □ No	□ Used Other MBE/DBE □ Used Non-MBE/DBE □ Self-performing

Name of Identified MBE/DBE Firm & MBE Classification	**Describe Item of Work Solicited**	**Initial Solicitation Date & Method**	**Follow-up Solicitation Date & Method**	**Details for Follow-up Calls**	**Quote Rec'd**	**Quote Used**	**Reason Quote Rejected**
Firm Name: **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American-Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification		Date: □ Mail □ Facsimile □ Email	Date: □ Phone □ Mail □ Facsimile □ Email	Time of Call: Spoke With: □ Left Message	□ Yes □ No	□ Yes □ No	□ Used Other MBE/DBE □ Used Non-MBE/DBE □ Self-performing

☐Please check if Additional Sheets are attached.

MDOT MBE/DBE FORM E
GOOD FAITH EFFORTS GUIDANCE AND DOCUMENTATION

Part 5 – Additional Information Regarding Rejected MBE/DBE Quotes

PAGE __ OF ___

Prime Contractor	Project Description	Solicitation Number

This form must be completed if Part 3 indicates that a MBE/DBE quote was rejected because the bidder/offeror is using a Non-MBE/DBE or is self-performing the Identified Items of Work. Provide the Identified Items Work, indicate whether the work will be self-performed or performed by a Non-MBE/DBE, and if applicable, state the name of the Non-MBE/DBE. Also include the names of all MBE/DBE and Non-MBE/DBE Firms that provided a quote and the amount of each quote.

Describe Identified Items of Work Not Being Performed by MBE/DBE (Include spec/section number from bid)	Self-performing or Using Non-MBE/DBE (Provide name)	Amount of Non-MBE/DBE Quote	Name of Other Firms who Provided Quotes & Whether MBE/DBE or Non-MBE/DBE	Amount Quoted	Indicate Reason Why MBE/DBE Quote Rejected & Briefly Explain
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non-MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other

Describe Identified Items of Work Not Being Performed by MBE/DBE (Include spec/section number from bid)	**Self-performing or Using Non-MBE/DBE (Provide name)**	**Amount of Non-MBE/DBE Quote**	**Name of Other Firms who Provided Quotes & Whether MBE/DBE or Non-MBE/DBE**	**Amount Quoted**	**Indicate Reason Why MBE/DBE Quote Rejected & Briefly Explain**
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE/DBE _____	$_____	_____ □ MBE/DBE □ Non- MBE/DBE	$_____	□ Price □ Capabilities □ Other

☐Please check if Additional Sheets are attached.

Attachment E. Veteran-Owned Small Business Enterprise (VSBE) Forms

This solicitation does not include a Veteran-Owned Small Business Enterprise goal.

Attachment F. Maryland Living Wage Affidavit of Agreement for Service Contracts

A. This contract is subject to the Living Wage requirements under Md. Code Ann., State Finance and Procurement Article, Title 18, and the regulations proposed by the Commissioner of Labor and Industry (Commissioner). The Living Wage generally applies to a Contractor or subcontractor who performs work on a State contract for services that is valued at $100,000 or more. An employee is subject to the Living Wage if he/she is at least 18 years old or will turn 18 during the duration of the contract; works at least 13 consecutive weeks on the State Contract and spends at least one-half of the employee's time during any work week on the State Contract.

B. The Living Wage Law does not apply to:

(1) A Contractor who:

(a) Has a State contract for services valued at less than $100,000, or

(b) Employs 10 or fewer employees and has a State contract for services valued at less than $500,000.

(2) A subcontractor who:

(a) Performs work on a State contract for services valued at less than $100,000,

(b) Employs 10 or fewer employees and performs work on a State contract for services valued at less than $500,000, or

(c) Performs work for a Contractor not covered by the Living Wage Law as defined in B(1)(b) above, or B (3) or C below.

(3) Service contracts for the following:

(a) Services with a Public Service Company;

(b) Services with a nonprofit organization;

(c) Services with an officer or other entity that is in the Executive Branch of the State government and is authorized by law to enter into a procurement ("Unit"); or

(d) Services between a Unit and a County or Baltimore City.

C. If the Unit responsible for the State contract for services determines that application of the Living Wage would conflict with any applicable Federal program, the Living Wage does not apply to the contract or program.

D. A Contractor must not split or subdivide a State contract for services, pay an employee through a third party, or treat an employee as an independent Contractor or assign work to employees to avoid the imposition of any of the requirements of Md. Code Ann., State Finance and Procurement Article, Title 18.

E. Each Contractor/subcontractor, subject to the Living Wage Law, shall post in a prominent and easily accessible place at the work site(s) of covered employees a notice of the Living Wage Rates, employee rights under the law, and the name, address, and telephone number of the Commissioner.

F. The Commissioner shall adjust the wage rates by the annual average increase or decrease, if any, in the Consumer Price Index for all urban consumers for the Washington/Baltimore metropolitan area, or any successor index, for the previous calendar year, not later than 90 days after the start of each fiscal year. The Commissioner shall publish any adjustments to the wage rates on the

Division of Labor and Industry's website. An employer subject to the Living Wage Law must comply with the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate, required by the Commissioner, automatically upon the effective date of the revised wage rate.

G. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's share of the health insurance premium, as provided in Md. Code Ann., State Finance and Procurement Article, §18-103(c), shall not lower an employee's wage rate below the minimum wage as set in Md. Code Ann., Labor and Employment Article, §3-413. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's share of health insurance premium shall comply with any record reporting requirements established by the Commissioner.

H. A Contractor/subcontractor may reduce the wage rates paid under Md. Code Ann., State Finance and Procurement Article, §18-103(a), by no more than 50 cents of the hourly cost of the employer's contribution to an employee's deferred compensation plan. A Contractor/subcontractor who reduces the wages paid to an employee based on the employer's contribution to an employee's deferred compensation plan shall not lower the employee's wage rate below the minimum wage as set in Md. Code Ann., Labor and Employment Article, §3-413.

I. Under Md. Code Ann., State Finance and Procurement Article, Title 18, if the Commissioner determines that the Contractor/subcontractor violated a provision of this title or regulations of the Commissioner, the Contractor/subcontractor shall pay restitution to each affected employee, and the State may assess liquidated damages of $20 per day for each employee paid less than the Living Wage.

J. Information pertaining to reporting obligations may be found by going to the Division of Labor and Industry website http://www.dllr.state.md.us/labor/prev/livingwage.shmtl and clicking on Living Wage for State Service Contracts.

F-1 Maryland Living Wage Requirements Affidavit of Agreement

Contract No. J02B8400024

Name of Contractor:

Address:

If the Contract Is Exempt from the Living Wage Law

The Undersigned, being an authorized representative of the above named Contractor, hereby affirms that the Contract is exempt from Maryland's Living Wage Law for the following reasons (check all that apply):

☐ Offeror is a nonprofit organization

☐ Offeror is a public service company

☐ Offeror employs 10 or fewer employees and the proposed contract value is less than $500,000

☐ Offeror employs more than 10 employees and the proposed contract value is less than $100,000

If the Contract Is a Living Wage Contract

A. The Undersigned, being an authorized representative of the above-named Contractor, hereby affirms its commitment to comply with Title 18, State Finance and Procurement Article, Annotated Code of Maryland and, if required, submit all payroll reports to the Commissioner of Labor and Industry with regard to the above stated contract. The Offeror agrees to pay covered employees who are subject to living wage at least the living wage rate in effect at the time service is provided for hours spent on State contract activities, and ensure that its subcontractors who are not exempt also pay the required living wage rate to their covered employees who are subject to the living wage for hours spent on a State contract for services. The Contractor agrees to comply with, and ensure its subcontractors comply with, the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate established by the Commissioner of Labor and Industry, automatically upon the effective date of the revised wage rate.

B. _____ (initial here if applicable) The Offeror affirms it has no covered employees for the following reasons: (check all that apply):

☐ The employee(s) proposed to work on the contract will spend less than one-half of the employee's time during any work week on the contract

☐ The employee(s) proposed to work on the contract is 17 years of age or younger during the duration of the contract; or

☐ The employee(s) proposed to work on the contract will work less than 13 consecutive weeks on the State contract.

The Commissioner of Labor and Industry reserves the right to request payroll records and other data that the Commissioner deems sufficient to confirm these affirmations at any time.

Name of Authorized Representative:

Signature of Authorized Representative : _____Date: _____

Title:

Witness Name (Typed or Printed) _____

Witness Signature: _____ Date: _____

SUBMIT THIS AFFIDAVIT WITH PROPOSAL

Attachment G. Federal Funds Attachments

This solicitation does not include a Federal Funds Attachment.

Attachment H. Conflict of Interest Affidavit and Disclosure

Reference COMAR 21.05.08.08

A. "Conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the State, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

B. "Person" has the meaning stated in COMAR 21.01.02.01B (64) and includes a bidder, offeror, contractor, consultant, or subcontractor or sub-consultant at any tier, and also includes an employee or agent of any of them if the employee or agent has or will have the authority to control or supervise all or a portion of the work for which a bid or offer is made.

C. The bidder or offeror warrants that, except as disclosed in §D, below, there are no relevant facts or circumstances now giving rise or which could, in the future, give rise to a conflict of interest.

D. The following facts or circumstances give rise or could in the future give rise to a conflict of interest (explain in detail—attach additional sheets if necessary):

E. The bidder or offeror agrees that if an actual or potential conflict of interest arises after the date of this affidavit, the bidder or offeror shall immediately make a full disclosure in writing to the procurement officer of all relevant facts and circumstances. This disclosure shall include a description of actions which the bidder or offeror has taken and proposes to take to avoid, mitigate, or neutralize the actual or potential conflict of interest. If the contract has been awarded and performance of the contract has begun, the Contractor shall continue performance until notified by the procurement officer of any contrary action to be taken.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By: _____

(Authorized Representative and Affiant

Attachment I. Non-Disclosure Agreement (TO Contractor)

THIS NON-DISCLOSURE AGREEMENT ("Agreement") is made by and between the State of Maryland (the "State"), acting by and through (Maryland Department of Transportation State Highway Administration) (the "Agency"), and _____ (the "TO Contractor").

RECITALS

WHEREAS, the TO Contractor has been awarded a contract (the "TO Agreement") following the solicitation for SHA APPLICATION PORTFOLIO BUSINESS SERVICES TORFP Solicitation # J02B8400024; and

WHEREAS, in order for the TO Contractor to perform the work required under the TO Agreement, it will be necessary for the State at times to provide the TO Contractor and the TO Contractor's employees, agents, and subcontractors (collectively the "TO Contractor's Personnel") with access to certain information the State deems confidential information (the "Confidential Information").

NOW, THEREFORE, in consideration of being given access to the Confidential Information in connection with the solicitation and the TO Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1. Regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such, "Confidential Information" means (1) any and all information provided by or made available by the State to the TO Contractor in connection with the TO Agreement and (2) any and all personally identifiable information (PII) (including but not limited to personal information as defined in Md. Ann. Code, General Provisions §4-101(h)) and protected health information (PHI) that is provided by a person or entity to the TO Contractor in connection with this TO Agreement. Confidential Information includes, by way of example only, information that the TO Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the TO Agreement.
2. The TO Contractor shall not, without the State's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information except for the sole and exclusive purpose of performing under the TO Agreement. The TO Contractor shall limit access to the Confidential Information to the TO Contractor's Personnel who have a demonstrable need to know such Confidential Information in order to perform under TO Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. The names of the TO Contractor's Personnel are attached hereto and made a part hereof as **Attachment I-2**. TO Contractor shall update **Attachment I-2** by adding additional names (whether TO Contractor's Personnel or a subcontractor's personnel) as needed, from time to time.
3. If the TO Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the TO Contractor's performance of the TO Agreement or will otherwise have a role in performing any aspect of the TO Agreement, the TO Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.
4. The TO Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, adopt or establish operating procedures and physical security measures, and take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties and to prevent all or any portion of the Confidential Information from falling

into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.

5. The TO Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the TO Contractor's Personnel or the TO Contractor's former Personnel. TO Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).
6. The TO Contractor shall, at its own expense, return to the Agency all Confidential Information in its care, custody, control or possession upon request of the Agency or on termination of the TO Agreement.
7. A breach of this Agreement by the TO Contractor or the TO Contractor's Personnel shall constitute a breach of the TO Agreement between the TO Contractor and the State.
8. TO Contractor acknowledges that any failure by the TO Contractor or the TO Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the TO Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The TO Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and seek damages from the TO Contractor and the TO Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the TO Contractor or any of the TO Contractor's Personnel to comply with the requirements of this Agreement, the TO Contractor shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and costs.
9. TO Contractor and each of the TO Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement, in no event less restrictive than as set forth in this Agreement, and the TO Contractor shall provide originals of such executed Agreements to the State.
10. The parties further agree that:
    a. This Agreement shall be governed by the laws of the State of Maryland;
    b. The rights and obligations of the TO Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State;
    c. The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information;
    d. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement;
    e. Signatures exchanged by facsimile are effective for all purposes hereunder to the same extent as original signatures;
    f. The Recitals are not merely prefatory but are an integral part hereof; and
    g. The effective date of this Agreement shall be the same as the NTP date of the TO Agreement entered into by the parties.

IN WITNESS WHEREOF, the parties have, by their duly authorized representatives, executed this Agreement as of the day and year first above written.

TO Contractor:	SHA
By: (seal)	By:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

I-2 NON-DISCLOSURE AGREEMENT

LIST OF CONTRACTOR'S EMPLOYEES AND AGENTS WHO WILL BE GIVEN ACCESS TO THE CONFIDENTIAL INFORMATION

Printed Name and Address of Individual/Agent	Employee (E) or Agent (A)	Signature	Date

I-3 NON-DISCLOSURE AGREEMENT

CERTIFICATION TO ACCOMPANY RETURN OR DELETION OF CONFIDENTIAL INFORMATION

I AFFIRM THAT:

To the best of my knowledge, information, and belief, and upon due inquiry, I hereby certify that: (i) all Confidential Information which is the subject matter of that certain Non-Disclosure Agreement by and between the State of Maryland and _____ ("TO Contractor") dated _____, 20_____ ("Agreement") is attached hereto and is hereby returned to the State in accordance with the terms and conditions of the Agreement; and (ii) I am legally authorized to bind the TO Contractor to this affirmation. Any and all Confidential Information that was stored electronically by me has been permanently deleted from all of my systems or electronic storage devices where such Confidential Information may have been stored.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF, HAVING MADE DUE INQUIRY.

DATE: _____

NAME OF TO CONTRACTOR: _____

BY: _____
(Signature)

TITLE: _____

Attachment J. HIPAA Business Associate Agreement

This solicitation does not require a HIPAA Business Associate Agreement.

Attachment K. Mercury Affidavit

This solicitation does not include the procurement of products known to likely include mercury as a component.

Attachment L. Location of the Performance of Services Disclosure

(submit with Proposal)

Pursuant to Md. Ann. Code, State Finance and Procurement Article, § 12-111, and in conjunction with the Proposal submitted in response to Solicitation No. J02B8400024, the following disclosures are hereby made:

1. At the time of Proposal submission, the Offeror and/or its proposed subcontractors:

___have plans

___have no plans

to perform any services required under the TO Agreement outside of the United States.

2. If services required under the contract are anticipated to be performed outside the United States by either the Offeror or its proposed subcontractors, the Offeror shall answer the following (attach additional pages if necessary):

a. Location(s) services will be performed:

_____
_____
_____

b. Reasons why it is necessary or advantageous to perform services outside the United States:

_____
_____
_____
_____
_____

The undersigned, being an authorized representative of the Offeror, hereby affirms that the contents of this disclosure are true to the best of my knowledge, information, and belief.

Date: _____

Offeror Name:

By: _____

Name:

Title:

Please be advised that the Agency may contract for services provided outside of the United States if: the services are not available in the United States; the price of services in the United States exceeds by an unreasonable amount the price of services provided outside the United States; or the quality of services in the United States is substantially less than the quality of comparably priced services provided outside the United States.

Attachment M. Task Order

CATS+ TORFP# J02B8400024 OF
MASTER CONTRACT #060B2490023

This Task Order Agreement ("TO Agreement") is made this day of Month, 2018 by and between _____ (TO Contractor) and the STATE OF MARYLAND, Maryland Department of Transportation State Highway Administration (SHA or the "Agency").

IN CONSIDERATION of the mutual promises and the covenants herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. In this TO Agreement, the following words have the meanings indicated:

   a. "Agency" means Maryland Department of Transportation State Highway Administration, as identified in the CATS+ TORFP # J02B8400024.

   b. "CATS+ TORFP" means the Task Order Request for Proposals # J02B8400024, dated MONTH DAY, YEAR, including any addenda and amendments.

   c. "Master Contract" means the CATS+ Master Contract between the Maryland Department of Information Technology and TO Contractor.

   d. "TO Procurement Officer" means <<TO Procurement Officer>>. The Agency may change the TO Procurement Officer at any time by written notice.

   e. "TO Agreement" means this signed TO Agreement between SHA and TO Contractor.

   f. "TO Contractor" means the CATS+ Master Contractor awarded this TO Agreement, whose principal business address is _____.

   g. "TO Manager" means Mark W Harrison. The Agency may change the TO Manager at any time by written notice to the TO Contractor.

   h. "TO Technical Proposal" means the TO Contractor's technical response to the CATS+ TORFP dated date of TO Technical Proposal.

   i. "TO Financial Proposal" means the TO Contractor's financial response to the CATS+ TORFP dated date of TO Financial Proposal.

   j. "TO Proposal" collectively refers to the TO Technical Proposal and TO Financial Proposal.

2. Scope of Work

2.1 This TO Agreement incorporates all of the terms and conditions of the Master Contract and shall not in any way amend, conflict with or supersede the Master Contract.

2.2 The TO Contractor shall, in full satisfaction of the specific requirements of this TO Agreement, provide the services set forth in Section 3 of the CATS+ TORFP. These services shall be provided in accordance with the Master Contract, this TO Agreement, and the following Exhibits, which are attached and incorporated herein by reference. If there is any conflict among the Master Contract, this TO Agreement, and these Exhibits, the terms of the Master Contract shall govern. If there is any conflict between this TO Agreement and any of these Exhibits, the following order of precedence shall determine the prevailing provision:

The TO Agreement,

Exhibit A – CATS+ TORFP

Exhibit B – TO Technical Proposal

Exhibit C – TO Financial Proposal

2.3 The TO Procurement Officer may, at any time, by written order, make changes in the work within the general scope of the TO Agreement. No other order, statement or conduct of the TO Procurement Officer or any other person shall be treated as a change or entitle the TO Contractor to an equitable adjustment under this Section. Except as otherwise provided in this TO Agreement, if any change under this Section causes an increase or decrease in the TO Contractor's cost of, or the time required for, the performance of any part of the work, whether or not changed by the order, an equitable adjustment in the TO Agreement price shall be made and the TO Agreement modified in writing accordingly. The TO Contractor must assert in writing its right to an adjustment under this Section within thirty (30) days of receipt of written change order and shall include a written statement setting forth the nature and cost of such claim. No claim by the TO Contractor shall be allowed if asserted after final payment under this TO Agreement. Failure to agree to an adjustment under this Section shall be a dispute under the Disputes clause of the Master Contract. Nothing in this Section shall excuse the TO Contractor from proceeding with the TO Agreement as changed.

3. Time for Performance

This TO Agreement is effective as of the date of Notice to Proceed (NTP). Unless terminated earlier as provided in the Master Contract the term of this TO Agreement is for a period of 5 years commencing on the NTP Date and terminating on the 5th anniversary thereof.

4. Consideration and Payment

4.1 The consideration to be paid the TO Contractor shall be done so in accordance with the CATS+ TORFP and shall not exceed $_____. Any work performed by the TO Contractor in excess of the not-to-exceed ceiling amount of the TO Agreement without the prior written approval of the TO Manager is at the TO Contractor's risk of non-payment.

4.2 Payments to the TO Contractor shall be made as outlined Section 3 of the CATS+ TORFP, but no later than thirty (30) days after the Agency's receipt of a proper invoice for services provided by the TO Contractor, acceptance by the Agency of services provided by the TO Contractor, and pursuant to the conditions outlined in Section 4 of this Agreement.

4.3 Each invoice for services rendered must include the TO Contractor's Federal Tax Identification Number which is _____. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1, of the State Finance and Procurement Article, Annotated Code of Maryland, as from time-to-time amended, are prohibited. Invoices must be submitted to the Agency TO Manager unless otherwise specified herein.

4.4 In addition to any other available remedies, if, in the opinion of the TO Procurement Officer, the TO Contractor fails to perform in a satisfactory and timely manner, the TO Procurement Officer may refuse or limit approval of any invoice for payment, and may cause payments to the TO Contractor to be reduced or withheld until such time as the TO Contractor meets performance standards as established by the TO Procurement Officer.

SIGNATURES ON NEXT PAGE

IN WITNESS THEREOF, the parties have executed this TO Agreement as of the date hereinabove set forth.

TO Contractor Name

_____ _____

By: Type or Print TO Contractor POC Date

Witness: _____

STATE OF MARYLAND, SHA

_____ _____

By: Peggy Tischler, TO Procurement Officer Date

Witness: _____

Approved for form and legal sufficiency this _____ day of _____ 20___.

_____

Assistant Attorney General

Attachment N. Certification Regarding Investments in Iran

Authority: State Finance & Procurement, §§17-701 – 17-707, Annotated Code of Maryland [Chapter 447, Laws of 2012.]

List: The Investment Activities in Iran list identifies companies that the Board of Public Works has found to engage in investment activities in Iran; those companies may not participate in procurements with a public body in the State. "Engaging in investment activities in Iran" means:

A. Providing goods or services of at least $20 million in the energy sector of Iran; or

B. For financial institutions, extending credit of at least $20 million to another person for at least 45 days if the person is on the Investment Activities In Iran list and will use the credit to provide goods or services in the energy of Iran.

The Investment Activities in Iran list is located at: www.bpw.state.md.us

Rule: A company listed on the Investment Activities In Iran list is ineligible to bid on, submit a proposal for, or renew a contract for goods and services with a State Agency or any public body of the State. Also ineligible are any parent, successor, subunit, direct or indirect subsidiary of, or any entity under common ownership or control of, any listed company.

NOTE: This law applies only to new contracts and to contract renewals. The law does not require an Agency to terminate an existing contract with a listed company.

CERTIFICATION REGARDING INVESTMENTS IN IRAN

The undersigned certifies that, in accordance with State Finance & Procurement Article, §17-705:

(i) it is not identified on the list created by the Board of Public Works as a person engaging in investment activities in Iran as described in §17-702 of State Finance & Procurement; and

(ii) it is not engaging in investment activities in Iran as described in State Finance & Procurement Article, §17-702.

The undersigned is unable make the above certification regarding its investment activities in Iran due to the following activities:

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Date: _____ Title: _____

Witness Name (Typed or Printed): _____

Witness Signature and Date: _____

Appendix 1. – Abbreviations and Definitions

For purposes of this TORFP, the following abbreviations or terms have the meanings indicated below:

A. Application Program Interface (API) - Code that allows two software programs to communicate with each other
B. Access - The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource
C. Business Day(s) – The official working days of the week to include Monday through Friday. Official working days excluding State Holidays (see definition of "Normal State Business Hours" below).
D. COMAR – Code of Maryland Regulations available on-line at http://www.dsd.state.md.us/COMAR/ComarHome.html.
E. Data Breach – The unauthorized acquisition, use, modification or disclosure of State data, or other Sensitive Data
F. Effective Date – Is the NTP Date, the date of mutual TO Agreement execution by the parties
G. Enterprise License Agreement (ELA) – An agreement to license the entire population of an entity (employees, on-site contractors, off-site contractors) accessing a software or service for a specified period of time for a specified value.
H. Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
I. Information Technology (IT) – All electronic information-processing hardware and software, including: (a) maintenance; (b) telecommunications; and (c) associated consulting services
J. Key Personnel – All TO Contractor Personnel identified in the solicitation as such that are essential to the work being performed under the Task Order. See TORFP **Section 3.10.5**.
K. Local Time – Time in the Eastern Time Zone as observed by the State of Maryland. Unless otherwise specified, all stated times shall be Local Time, even if not expressly designated as such.
L. Maryland Department of Transportation State Highway Administration or (SHA or the "Agency")
M. Minority Business Enterprise (MBE) – Any legal entity certified as defined at COMAR 21.01.02.01B (54) which is certified by the Maryland Department of Transportation under COMAR 21.11.03.
N. Normal State Business Hours - Normal State business hours are 8:00 a.m. – 5:00 p.m. Monday through Friday except State Holidays, which can be found at: www.dbm.maryland.gov – keyword: State Holidays.
O. Notice to Proceed (NTP) – A written notice from the TO Manager that work under the Task Order, project or Work Order (as applicable) is to begin as of a specified date. The NTP Date is the start date of work under the Task Order, project or Work Order. Additional NTPs may be issued by the TO Manager regarding the start date for any service included within this solicitation with a delayed or non-specified implementation date.

P. NTP Date – The date specified in a NTP for work on Task Order, project or Work Order to begin.
Q. Offeror – A Master Contractor that submits a Proposal in response to this TORFP.
R. Personally Identifiable Information (PII) – Any information about an individual maintained by the State, including (1) any information that can be used to distinguish or trace an individual identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
S. Protected Health Information (PHI) – Information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
T. Security Incident – A violation or imminent threat of violation of computer security policies, Security Measures, acceptable use policies, or standard security practices. "Imminent threat of violation" is a situation in which the organization has a factual basis for believing that a specific incident is about to occur.
U. Security or Security Measures – The technology, policy and procedures that a) protects and b) controls access to networks, systems, and data
V. Sensitive Data - Means PII;PHI; other proprietary or confidential data as defined by the State, including but not limited to "personal information" under Md. Code Ann., Commercial Law § 14-3501(d) and Md. Code Ann., St. Govt. § 10-1301(c) and information not subject to disclosure under the Public Information Act, Title 4 of the General Provisions Article; and .information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information
W. Software - The object code version of computer programs licensed pursuant to this TO Agreement. Embedded code, firmware, internal code, microcode, and any other term referring to software that is necessary for proper operation is included in this definition of Software. Software includes all prior, current, and future versions of the Software and all maintenance updates and error corrections. Software also includes any upgrades, updates, bug fixes or modified versions or backup copies of the Software licensed to the State by TO Contractor or an authorized distributor.
X. Solution - All Software, deliverables, services and activities necessary to fully provide and support the TORFP scope of work. This definition of Solution includes all System Documentation developed as a result of this TO Agreement. Also included are all Upgrades, patches, break/fix activities, enhancements and general maintenance and support of the Solution and its infrastructure.
Y. State – The State of Maryland.
Z. Source Code – Executable instructions for Software in its high level, human readable form which are in turn interpreted, parsed and/or compiled to be executed as part of a computing system.

AA. System Availability – The period of time the Solution works as required excluding non-operational periods associated with planned maintenance.

BB. System Documentation – Those materials necessary to wholly reproduce and fully operate the most current deployed version of the Solution in a manner equivalent to the original Solution including, but not limited to:

1) Source Code: this includes source code created by the TO Contractor or subcontractor(s) and source code that is leveraged or extended by the TO Contractor for use in the Task Order.
2) All associated rules, reports, forms, templates, scripts, data dictionaries and database functionality.
3) All associated configuration file details needed to duplicate the run time environment as deployed in the current deployed version of the system.
4) All associated design details, flow charts, algorithms, processes, formulas, pseudo-code, procedures, instructions, help files, programmer's notes and other documentation.
5) A complete list of Third Party, open source, or commercial software components and detailed configuration notes for each component necessary to reproduce the system (e.g., operating system, relational database, and rules engine software).
6) All associated user instructions and/or training materials for business users and technical staff, including maintenance manuals, administrative guides and user how-to guides.
7) Operating procedures

CC. Task Order (TO) – The scope of work described in this TORFP.

DD. TO Agreement - The contract awarded to the successful Offeror pursuant to this Task Order Request for Proposals, the form of which is attached to this TORFP as **Attachment M.**

EE. TO Contractor Personnel - Employees and agents and subcontractor employees and agents performing work at the direction of the TO Contractor under the terms of the Task Order awarded from this TORFP.

FF. TO Proposal – As appropriate, either or both of an Offeror's TO Technical or TO Financial Proposal.

GG. Technical Safeguards – The technology and the policy and procedures for its use that protect State Data and control access to it.

HH. Third Party Software – Software and supporting documentation that:

8) are owned by a third party, not by the State, the TO Contractor, or a subcontractor,
9) are included in, or necessary or helpful to the operation, maintenance, support or modification of the Solution; and
10) were specifically identified and listed as Third Party Software in the Proposal.

II. Total Proposal Price - The Offeror's total proposed price for services in response to this solicitation, included in the TO Financial Proposal with **Attachment B** – TO Financial Proposal Form, and used in the financial evaluation of Proposals (see TORFP **Section 5.5**).

JJ. Veteran-owned Small Business Enterprise (VSBE) – A business that is verified by the Center for Verification and Evaluation (CVE) of the United States Department of

Veterans Affairs as a veteran-owned small business. See Code of Maryland Regulations (COMAR) 21.11.13.

KK. Work Order– A subset of work authorized by the TO Manager performed under the general scope of this TORFP, which is defined in advance of TO Contractor fulfillment, and which may not require a TO Agreement modification. Except as otherwise provided, any reference to the Task Order shall be deemed to include reference to a Work Order.

Appendix 2. – Offeror Information Sheet

Offeror	
Company Name	
Street Address	
City, State, Zip Code	
TO Contractor Federal Employer Identification Number (FEIN)	
TO Contractor eMM ID number	As of the date of Proposal submission, are you registered to do business with the state of Maryland?
SBE / MBE/ VSBE Certification	
SBE	Number: Expiration Date:
VSBE	Number: Expiration Date:
MBE	Number: Expiration Date: Categories to be applied to this solicitation (dual certified firms must choose only one category).
Offeror Primary Contact	
Name	
Title	
Office Telephone number (with area code)	
Cell Telephone number (with area code)	
e-mail address	
Authorized Offer Signatory	
Name	
Title	
Office Telephone number (with area code)	
Cell Telephone number (with area code)	
e-mail address	

Appendix 3. - Labor Classification Personnel Resume Summary

INSTRUCTIONS:

1. For each person proposed, complete one Labor Category Personnel Resume Summary to document how the proposed person meets each of the minimum requirements.

   For example: If you propose John Smith, who is your subcontractor, and you believe he meets the requirements of the Group Facilitator, you will complete the top section of the form by entering John Smith's name and the subcontractor's company name. You will then complete the right side of the Group Facilitator form documenting how the individual meets each of the requirements. Where there is a time requirement such as three months experience, you must provide the dates from and to showing an amount of time that equals or exceeds mandatory time requirement; in this case, three months.

2. Additional information may be attached to each Labor Category Personnel Resume Summary that may assist a full and complete understanding of the individual being proposed.

3. For this TORFP,

   A. Master Contractors shall comply with all personnel requirements defined under the Master Contract RFP 060B2490023.
   B. Master Contractors shall propose the CATS+ Labor Category that best fits each proposed resource. A Master Contractor may only propose against labor categories in the Master Contractor's CATS+ Master Contract Financial Proposal.
   C. A Master Contractor's entire TO Technical Proposal will be deemed not susceptible for award if any of the following occurs:
      1) Failure to follow these instructions.
      2) Failure to propose a resource for each job title or labor category identified in the TORFP as a required submission.
      3) Failure of any proposed resource to meet minimum requirements as listed in this TORFP and in the CATS+ Master Contract.
      4) Placing content on the **Minimum Qualifications Summary** that is not also on the **Personnel Resume Summary**. *The function of the **Minimum Qualifications Summary** is to aid the agency to make a minimum qualification determination. Information on the **Minimum Qualification Summary** must correspond with information on the **Personnel Resume Summary** and shall not contain additional content not found on the other form.*

4. Complete and sign the **Minimum Qualifications Summary (Appendix 3A)** and the **Personnel Resume Form (Appendix 3B)** for each resource proposed. Alternate resume formats are not allowed.

   a. The **Minimum Qualifications Summary** demonstrates the proposed resource meets minimum qualifications for the labor category, as defined in the CATS+ RFP Section 2.10, and any additional minimum requirements stated in this TORFP. For each minimum qualification, indicate the location on the **Personnel Resume Form (Appendix 3B)** demonstrating meeting this requirement.

      Only include the experience relevant to meeting a particular minimum qualification. Every skill must be linked to specific work experience and/or education. The **Minimum**

Qualification Summary shall not contain content that cannot be correlated to the **Personnel Resume Summary**.

Every experience listed on the **Minimum Qualifications Resume Summary** must be explicitly listed with start and stop dates. Where there is a time requirement such as three months' experience, you must provide the dates from and to showing an amount of time that equals or exceeds the mandatory time requirement; in this case, three months. Note: Overlapping time periods shall only count once against a specific minimum qualification (i.e., a minimum qualification may not be met by listing two examples occurring during the same time period.).

b. The **Personnel Resume Form** provides resumes in a standard format. Additional information may be attached to each **Personnel Resume Summary** if it aids a full and complete understanding of the individual proposed.

3A. MINIMUM QUALIFICATIONS SUMMARY

CATS+ TORFP # J02B8400024

All content on this form must also be on the Personnel Resume Form.
ONLY include information on this summary that supports meeting a minimum qualification.

Proposed Key Personnel:	Master Contractor:			CATS+ Labor Category:	
Education: (Insert the education requirements for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP	Institution/Address:			Degree or Certification: Field of Study:	Year Completed:
Generalized Experience: (Insert the generalized experience description for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP)	Start	End	Company/Job Title	Relevant Work Experience	
Specialized Experience: (Insert the specialized experience description for the proposed labor category from Section 1.1 and 2.10 of the CATS+ RFP)	Start	End	Company/Job Title	Relevant Work Experience	
TORFP Additional Requirements **(Insert, if applicable, the additional requirements from Section 3.10.3)**					

The information provided on this form for this labor category is true and correct to the best of my knowledge:

Master Contractor Representative:	Proposed Key Personnel:
Signature	Signature
Printed Name:	Printed Name
Date	Date

Sign each Form

3B. Labor Classification Personnel Resume Summary

TORFP # J02B8400024

Instructions: Enter resume information in the fields below; do not submit other resume formats. Submit one resume for each proposed resource

Candidate Name:	
TO Contractor:	(offeror CompanyName)

Education / Training

Institution Name / City / State	Degree / Certification	Year Completed	Field Of Study
<add lines as needed>			

Relevant Work Experience

Describe work experience relevant to the Duties / Responsibilities and Minimum Qualifications described in the TORFP. Starts with the most recent experience first; do not include non-relevant experience.

[Organization] [Title / Role] [Period of Employment / Work] [Location] [Contact Person (Optional if current employer)]	Description of Work…
[Organization] [Title / Role] [Period of Employment / Work] [Location] [Contact Person]	Description of Work…
<add lines as needed>	

Employment History

List employment history, starting with the most recent employment first

Start and End Dates	Job Title or Position	Organization Name	Reason for Leaving
<add lines as needed>			

Personnel Resume Summary (Continued)

*"Candidate Relevant Experience" section must be filled out. Do not enter "see resume" as a response.

References

List persons the State may contact as employment references

Reference Name	Job Title or Position	Organization Name	Telephone / E-mail
<add lines as needed>			

Proposed Individual's Name/Company Name:	How does the proposed individual meet each requirement?
LABOR CATEGORY TITLE:	*Offeror to Enter the Labor Category Name*
Requirement (See Section 2.10 of the CATS+ Master Contract)	Candidate Relevant Experience *
Education: [Insert the education description from Section 2.10 of the CAST+ Master Contract for the applicable labor category]	Education:
Experience: [Insert the experience description from Section <<x.x>>for the applicable labor category]	Experience:
Duties: [Insert the duties description from Section <<x.x>>for the applicable labor category]	Duties:

The information provided on this form for this labor category is true and correct to the best of my knowledge:

TO Contractor Representative:	Proposed Individual:
Signature	Signature
Printed Name:	Printed Name
Date	Date

Sign each Form

Appendix 4 – Criminal Background Check Affidavit

AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the _____(Title)_____ and the duly authorized representative of ___(Master Contractor)_____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

I hereby affirm that ____ (Master Contractor) _____ has complied with Section 2.4, Security Requirements of the Department of Information Technology's Consulting Technical Services Master Contract Number 060B2490023 (CATS+) hereto as Exhibit A.

I hereby affirm that the ____ (Master Contractor)_____ has provided Maryland Transportation Authority with a summary of the security clearance results for all of the candidates that will be working on Task Order MICROSOFT DYNAMICS SL SOFTWARE TECHNICAL AND USER SUPPORT J02B8400024 and all of these candidates have successfully passed all of the background checks required under Section 2.4.3.2 of the CATS + Master Contract. Master Contractors hereby agrees to provide security clearance results for any additional candidates at least seven (7) days prior to the date the candidate commences work on this Task Order.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

_____

Master Contractor

_____

Typed Name

_____

Signature

_____

Date

This for is due within 30 days of notice of award

Appendix 5 - Maryland Department of Transportation Information Security Plan

See separate Attachment

Appendix 6 Weekly TO Contractor Personnel Status Report

Weekly Status Report

Week Starting: <<week starts on a Monday>>	**Date: <<date prepared mm/dd/yyyy>>**
Report Prepared by: <<TO Contractor Personnel>>	**Task Number: J02B3400049**
TO Contractor: <<name of the TO Contractor>>	
Task Name: SHA Business Application Portfolio Business Services Task Order	

Name	Labor Category	Hours Expended for the
<<TO Contractor Personnel>>	<<labor category name associated with TO Contractor Personnel>>	<<##.#>>

ACTIVITIES COMPLETED:

<<Activity 1 Name>> ***(##.# Hours)***

- <<activity task 1>>
- <<activity task 2>>
- <<activity task 3>>
- <<activity task 4>>

Administrative ***(##.# Hour)***

- <<activity task 1>>
- <<activity task 2>>
- <<activity task 3>>

ACTIVITIES IN PROGRESS:

- <<Activity 1 Name>>

NEXT WEEK PLANNED ACTIVITIES

- <<activity 1 description>>

ACTIVITIES ON HOLD/ISSUES:

- <<Activity/Issue>>

ACTIVITIES REQUIRING OVERTIME AND TIME USED:

Date	Hours	Comments

ACTION ITEMS:

Item	Status	Comments

Appendix 7 - CERTIFICATION REGARDING DISCRIMINATORY BOYCOTTS OF ISRAEL

Authority: Executive Order 01.01.2017.25 (issued October 23, 2017)

☐ The undersigned offeror hereby certifies and agrees that the following information is correct:

In preparing its proposal on this project, the offeror has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not, in the solicitation, selection, or commercial treatment of any subcontractor, vendor, or supplier, refused to transact or terminated business activities, or taken other actions intended to limit commercial relations, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel and its territories. The offeror also has not retaliated against any person or other entity for reporting such refusal, termination, or commercially limiting actions. Without limiting any other provision of the solicitation for this project, it is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the proposal submitted by the offeror on this project, and terminate any contract awarded based on the bid.

☐ The undersigned is unable make the above certification regarding boycotts of Israel due to the following activities:

_____

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS CERTIFICATION ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Date: _____ Title:_____

Appendix 5

MARYLAND DEPARTMENT OF TRANSPORTATION

INFORMATION SECURITY PLAN

Revision Date: 05/05/2017

Table of Contents

This document contains sensitive information; its contents are not to be shared without the written permission of the Maryland Department of Transportation Chief Information Officer.

1.1 Objective of Security Planning

The objective of system security planning is to improve protection of information technology (IT) resources. Maryland Department of Transportation (MDOT) systems have some level of sensitivity and require protection as part of good management practice. This document discusses the protection of MDOT information technology (IT) resources. The content provides security guidance in the form of subject matter security policies grouped together to form a basis for a security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

The purpose of this security plan is to provide an overview of the security requirements for the MDOT tangible and intangible assets. This document provides security guidance for security controls that are in place or are planned in order to strengthen the MDOT overall security posture. This system security plan also delineates responsibilities and expected behavior of all individuals who access MDOT IT resources. The intent of this security plan is to provide a living document that should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for use by all MDOT Agencies and departments and reflects input from various MDOT managers with responsibilities for various IT resources. Additional contributors include MDOT information owners, system administrators, system operators, end-users, and the Security Working Group for the MDOT. Updated information may be included in the basic plan and the structure and format will continue to be organized according to MDOT agency requirements as defined by the MDOT Security Working Group (SWG) beginning in early 2000.

This security plan will protect MDOT IT resources, if all Transportation Business Units (TBUs) of the MDOT review and continue to contribute requirements to the Security Working Group where necessary changes are authorized. All security relevant enhancements must be documented and authorized by the MDOT Change Advisory Board (CAB)on a weekly basis. This risk management component of MDOT provides an important quality control by authorizing proposed change control and accepting all residual risks ensuring a balance among continuity of operations, costs, and viable security solutions.

> **The security-planning document is based on an assessment of management, operational and technical controls and the authorization of the CAB in response to recommendations from modal representatives and the Security Working Group. An annual review of the entire security plan must be done and documented and a periodic recurring review of the guidance provided within this security plan must be carried out in response to any significant change that impacts the three main security attributes, namely, confidentiality, integrity, and availability. This security plan better positions the MDOT in ongoing efforts to strengthen security posture, and meeting fiduciary responsibility of due care and due diligence. Thus, MDOT is**

taking a proactive approach to information assurance through layered security that calls upon talent, technology, and tools.

1.2 History of This Document

The Information Systems Security Plan document is the result of a collaborative effort between the MDOT modal representatives and the SWG and is based on the requirements of the MDOT TBUs as submitted to the SWG. Work continues in crafting content and enhancing structure and format that complements existing MDOT documentation. Adoption of this document is contingent upon acceptance by the MDOT Change Advisory Board.

1.3 Organization of This Document

Security Policy is the basis for much of the security guidance within an organization, therefore this document is organized in a linear format with the subject matter content reflecting various specific security policies contributed from MDOT representatives. The SWG considered the content and appropriateness before making further changes during review sessions held monthly and the policies will eventually be available on MDOT intranet web sites for easy access.

1.4 Seven Areas of Security Useful For Policy and Planning

1.4.1 Physical Security

Physical security measures focus on the physical protection of a system or facility and the controls in place, which restrict access to system resources through:

- Access control systems that range from simple key locks to cipher locks and sophisticated key/swipe card systems, and biometric fingerprint readers.
- Keys, combinations and keycards that require the same level of protection afforded the most sensitive information processed or handled within the facility.

1.4.2 Environmental Security

- Fire suppression systems (sprinklers, fire extinguishers).
- Heating and air conditioning systems.
- Emergency lighting and power distribution systems.
- Controlled environment (temperature, humidity, air filtration).
- Manual procedures and practices designed to protect delicate equipment from damage.
- Prohibition of eating and drinking around computer equipment.

- Prohibition of smoking around equipment to eliminate a common source of damage to hard drives and potential for fires.

- Institution of good housekeeping practices to control dust and dirt around computer equipment.

1.4.3 Personnel Security

Personnel security practices are those steps taken to:

- Ensure the integrity and reliability of prospective system users and all other persons with access to sensitive infrastructure and information.

- Ensure user awareness and understanding of their individual security responsibilities.

1.4.4 Hardware Security

- Ensure the protection of the hardware components of a system.

- Maintenance of accurate and up-to-date inventories of all equipment.

- Procedures (property passes) that ensure accountability for all equipment.

- Procedures for securing or logically disconnecting equipment when idle or unattended

1.4.5 Software And Data Security

Security practices in these two areas focus on the manual practices and procedures implemented to complement the automated security controls that:

- Protect operating system software, applications software and database files.

- Protect (configuration/change management) application and operating system software throughout the development and integration processes.

- Provide assurance of the integrity and accuracy of the software.

- Continue software and data security practices throughout the system life cycle.

- Address the effective implementation, integration and administration of the various security features contained in the operating system, application, and database software.

1.4.6 Security Administration

Security administration practices include those measures associated with the implementation and administration of the computer security program. These practices include:

- Develop and implement comprehensive and effective security plans.
- Develop and test contingency and disaster recovery plans.
- Document all aspects of the security program.
- Develop and provide security training to all employees at all levels.
- Maintain a high level of user security awareness.

1.4.7 Procedural Security

Procedural security measures include manual controls implemented to supplement automated protection provided by infrastructure components by:

- Documentation of those measures and controls as a foundation to support secure system operations.
- Creation of an enterprise level Security Policy document that is based on a security risk assessment baseline that provides guidance for the creation of subsequent security documentation and supporting procedures.
- Includes the definitions, roles and responsibilities of all system users.
- Specifies the system security architecture and implementation.
- Specifies types of user activities.
- Describes other sets of manual procedures designed to ensure the safe and secure operation of networks and mainframe systems.

Section 2: Introduction

2.1 Critical Business Function

Information and information systems are necessary for the performance of just about every essential activity. Serious security problems with this information or these information systems could result in lost customers, reduced revenues, identity theft, compromise of data, and/or degraded reputation. As a result, information security must be a critical part of an MDOT's business environment.

2.2 Information Security Policies

An Information Security Policy is an imperative element of a complete information security plan that touches every part of MDOT where data is created, modified, stored or processed. Internet security demands the presence of policies that dictate how security products and devices are used to protect MDOT assets. Information Security is not about tools, but about risk assessment, management, and everyone exercising best practices. Therefore, sound security policies and practices help shore up defenses and thwart inadvertent or hostile attacks on the MDOT network. Adequate Information Security Policies that secure MDOT services creates trustworthiness that customers both demand and deserve.

Section 3: Remote Data Access Policy

3.1 Purpose

The purpose of this policy is to support the appropriate strategies for, and acceptable use of, remote access to Maryland Department of Transportation (MDOT) networks and network services and MDOT data. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT Chief Information Officer (CIO).

3.2 Scope

This policy applies to an individual, group of individuals, organizations, or companies who have been given authorization to access the Maryland Department of Transportation (MDOT) enterprise network/data remotely. This policy applies to all Transportation Business Units (TBUs), Agencies and/or Departments operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy follow a structured review and approval process.

For the purpose of this policy, Remote Access is defined as accessing non-public MDOT or TBU networks, computers, or computer services and applications (such as Web sites and Web-based applications and corporate data from a location that does not provide a direct connection (wired or wireless) to the MDOT/TBU Enterprise (internal) network/data. If at any time the connection must go through a network not provided by MDOT, the connection is considered remote access.

Public access to services, data, and applications made available on the Internet is not within the scope of this policy.

3.3 Policy Statement

Remote access is made available for administrative, management, enforcement, procurement, support, and maintenance functions. MDOT computers and networks provide access to numerous computing resources, many of which contain confidential data or contain devices that support public safety. Remote access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations. Users must also ensure the appropriate confidentiality of information retrieved and stored on remote devices.

.

3.4 Responsibilities

Each TBU is responsible for observing this policy or developing policy that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "Criminal Justice Information System (CJIS) Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

Remote Data Access Policy is developed by the MDOT sanctioned Security Working Group and submitted to Configuration Control Change Advisory Board (CAB) for interim approval. The MDOT CIO will present the proposed policy to the Information Technology Governance Board (ITGB) for review. The MDOT CIO will have final approval of the policy.

Approved Remote Data Access Policy is implemented under the direction of the MDOT Network Project Manager and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

The following sections define remote access responsibilities based on the role of the individual:

3.4.1 MDOT

MDOT will provide and centrally manage a Mobile Device Management Suite (MDM)[1]. This suite will enable technical controls to be managed on remote devices by MDOT. The MDM suite will force specific security functionality on remote devices such as password locks/timeouts, etc… At any time MDOT may find it necessary for security reasons to deregister a remote device, thereby cutting off access to the MDOT network. The above described functionality covers both personally owned and state owned equipment.

3.4.2 Remote Access User

Remote Access Users are defined as individual employees, contractors, or federal/state/local government employees who require remote access to MDOT networks and network services and corporate data. Remote Access Users are responsible for obtaining, completing, submitting, and observing requirements of the Remote Access Request Form.

[1] As of this update 01/09/14 An MDM suite has been purchased. TBU administrators have been trained and will be able to establish their policies for applications that would be available from mobile devices.

All Internet Remote Access Users are responsible for procuring, configuring, and installing a personal firewall, anti-virus protection software, and encryption software (as appropriate for sensitive data) on the device used to remotely connect to MDOT, if available. Remote Access Users are further responsible for keeping these protections up to date. Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities. Remote Users accept that their personally owned or MDOT provided mobile device will be managed via the MDM system. MDOT will load MDM software which allows MDOT the ability to remote disconnect and even wipe the device of MDOT info that is segmented out separately from their own information if it is a personal device.

The Remote Access User is responsible for installing, configuring, and maintaining any additional software required for establishing remote access communications, such as Virtual Private Network (VPN) clients or Secure Socket Layer (SSL) clients. Remote Access Users are also responsible for any additional software required to access network services, such as Citrix or other required software on their personal device.

The Remote Access User is responsible for the safekeeping of any devices assigned to the user for two-factor authentication, (such as hardware tokens mini-token, smart cards, etc.) and must report lost or stolen devices immediately to their Remote Access Administrator or TBU Service Desk. The Remote Access User may incur the cost of replacement devices.

The Remote Access User is responsible for reporting Remote Access Client or Application Software problems to their TBU Service Desk. The Remote Access User is also responsible for notifying the Remote Access Administrator that the connection either does or does not work upon completion of installation.

The Remote Access User is responsible for all system hardware and software maintenance to their remote device. MDOT and MDTA are not responsible for the condition of the remote Access User's personal remote device.

The Remote Access User's supervisor is responsible for notifying the Remote Access Administrator if and when the Remote Access User leaves state service, or is no longer working on behalf of an MDOT TBU in the case of a contractor.

3.4.3 TBU Supervisor

The TBU Supervisor is responsible for reviewing the Remote Access Request Form from the User and ensuring the user has correctly completed and signed the user portion of the form.

The TBU Supervisor authorizes the request by signing the Remote Access Request Form and specifying the types of access the User is granted. The TBU Supervisor then forwards the form to the TBU IT Office.

The TBU Supervisors will use MDOT approved technologies such as MDM, virtualization and remote control, to keep confidential data off mobile devices.

3.4.4 TBU Remote Access Administrator

The TBU Remote Access Administrator is responsible for coordinating activities associated with the Remote Access Request Form. He/she ensures the information on the form is correct and signed by the User, and the User's supervisor.

The TBU Remote Access Administrator is responsible for creating a remote access account for the user.

The TBU Remote Access Administrator is responsible for providing the User with all the passwords, configuration information, installation software and manuals required to access resources on the MDOT network remotely.

The TBU Remote Access Administrator is responsible for providing any required training to the Remote Access User on the use of applications required for Remote Access to the MDOT network

Each TBU Remote Access Administrator shall maintain a file, electronic or paper, containing the signed copies of the Remote Access Forms.

The Remote Access Administrator is responsible for notifying the user's supervisor when the account is setup.

The Remote Access Administrator is responsible for notifying the Remote Access User's Supervisor of violations of this and any acceptable use policy.

3.4.5 Remote Access Request Process

Figure 1 presents a diagram of the remote access request process.

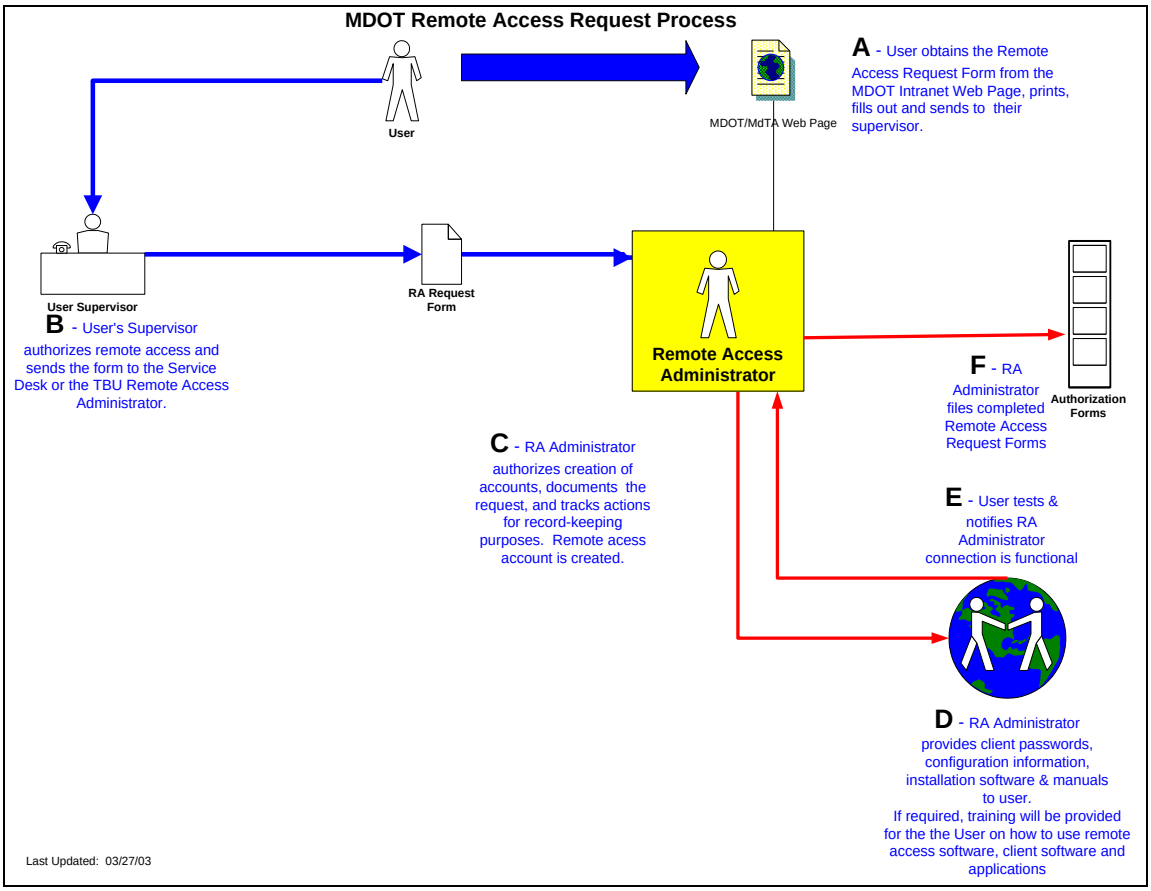

Figure 1 - Remote Access Request Process

3.5 Guidance

3.5.1 User or Individual Remote Access

An MDOT/TBU employee or individual contractor employee (User) requiring remote access to the MDOT/TBU network(s) and services initiates the Remote Access Request Process. The entity can obtain the Remote Access Request Form from the MDOT Intranet Web Page) or from the Remote Access Administrator. The User will print, complete and sign the User portion of the form and forward it to the User's Supervisor.

The User's Supervisor will review the User's request, authorize it and send the MDOT Remote Access Request Form to the TBU Service Desk or Remote Access Administrator.

The TBU Remote Access Administrator then reviews the request, ensures the Supervisor has correctly completed the Supervisor's section. The TBU Remote Access Administrator will ensure the request is documented and the actions are tracked in Maximo or another process for record-keeping purposes.

The TBU Remote Access Administrator then creates a remote access account for the user.

The TBU Remote Access Administrator maintains a file, electronic or paper, containing the completed MDOT Remote Access Request Form.

3.5.2 Third Party Remote Access

Request for remote access from organizations seeking a site-to-site connection over Internet-based Virtual Private Network (VPN) connections, or via direct telecommunication circuits will follow the guidance found in the "Third-party Access Policy".

3.5.3 Acceptable Use

Remote Access is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards activities;
- Communications for administrative purposes.
- Activities involved in the remote administration, support, or maintenance of MDOT/TBU network, computers, applications, and computing services
- Remote access to authorized systems and or data via the Internet

3.5.4 Remote Host Requirements for PCI Data Security Standards

In accordance with Payment Card Industry Data Security Standards (PCI DSS)[2], any MDOT employee or contractor remotely accessing a device that is in-scope with cardholder data must use a State-issued laptop with the following configuration in effect:

[2] PCI DSS Requirements and Security Assessment Procedures v3., 1.4, 1.4a, 1.4b (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf)

- Local firewall configured according to MDOT standards that cannot be changed by the laptop user.

- Local administrator account is not known or accessible by the laptop user.

- Local user account is for use by the laptop user and does not have access to change the firewall settings.

- Automatic updates setup for anti-virus, malware, and patches.

3.5.5 Restrictions

Remote Access may not be used for unlawful activities, commercial purposes not under the auspices of MDOT, personal financial gain, personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Remote Access:

- Private or personal, for profit activities (e.g., consulting for pay, sale of goods, charity fundraising);

- Solicitation of non-State business, or any use for personal gain or profit;

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

- At no time should any MDOT employee, contractor, or federal/state/local government employee provide their login or email password to anyone, not even family members.

- MDOT employees, contractors or federal/state/local government employee with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to the MDOT corporate network, is not connected to any other network at the same time

- Accessing or transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;

- Use for any purpose that is against State or Public policy or contrary to the State's best interest;

- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;

- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted

- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

- Misrepresenting in any manner, your identity, your account or a computing device in an Email or other electronic communication;

- Sending chain letters, advertisements, or solicitations of any type;

- Sending mass mailings to individuals who have not expressly agreed to be contacted in this manner;

- Knowingly sharing a personal account which includes use of a two-factor authentication device such as a token, grid card, soft token, etc.;

- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;

- Disclosing confidential or proprietary information.

- Use of any Dial-in desktop modems is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of remote control software is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of a network monitoring tool is prohibited unless specifically approved through the MDOT Change process-(CAB) Change Advisory Board

3.5.6 Representation

Remote Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

3.5.7 Interference

Remote Access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Remote Access systems. Such uses include, but are not limited to chain letters, "spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

3.5.8 No Expectation of Privacy

Privacy of Remote Access is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent, or received using the State's email system to authorized State supervisory personnel. The State affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations. The State shall make every reasonable effort to avoid viewing Union-related messages initiated by Union staff or bargaining unit members in accordance with Union agreements.

3.5.9 Security

The following specific guidance relating to Remote Access security is provided:

Strong Authentication

All users connecting from a remote host to the internal enterprise network must use two-factor authentication employing a method tested and approved by the Security Working Group.

VPN Encryption

All users connecting from a remote host to the internal enterprise network must use an encryption method that has been tested and approved by the Remote Access Group.

Virus Scan Software and Personal Firewalls

All users connecting from a remote host to the internal enterprise network must procure, install, and operate personal anti-virus and malware protection software. All users connecting from a remote host to the internal enterprise network via the Internet must procure, install and operate personal firewall software. Users should consult the INFOSEC group for guidance on acceptable approaches.

Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities.

All users connecting from a remote host to the internal enterprise network may be subject to a coordinated vulnerability assessment by MDOT or upon MDOT direction of their security contractor to test for proper security implementation at the remote host.

Authentication Token Policy

All users in possession of a security token are responsible for guarding and insuring the safekeeping of their token and must not share or redistribute tokens.

Users must report lost or stolen tokens to the remote access administrator or TBU Service Desk immediately. In the event a token is stolen, a police report must be filed for the missing article.

VPN Client Updates

VPN client updates are distributed to each TBU Remote Access Administrator and become the TBU Remote Access Administrator responsibility to distribute the update to their users.

Disclaimer

MDOT assumes no responsibility for any hardware, software, operating system problems, or the loss of any functionality or data to any personal user device used by any MDOT TBU Remote Access User.

3.5.10 Records Retention

State Records communicated using Remote Access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Remote Access system in accordance with each Department's standard practices.

Examples of Remote Access messages that typically are records include:

- Policies and directives,
- Correspondence or memoranda related to official business,

- Work schedules and assignments,
- Agendas and minutes of meetings,
- Drafts of documents that are circulated for comment or approval,
- Any document that initiates, authorizes, or completes a business transaction,
- Final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- Personal messages and announcements,
- Copies or extracts of documents distributed for convenience or reference,
- Phone message slips,
- Announcements of social events

Records communicated via Remote Access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

3.6 Definitions and Terminology

The following table defines the terms used to describe the various devices, entities or groups within this document.

The Network or Enterprise Network	MDOT and TBU network components.
Remote Access User	MDOT or TBU Employee/Contractor or Government Employee who has a job related/defined requirement to access the MDOT and TBU networks from a remote location.
Internet Users	Any remote access user connecting to the Enterprise network via an Internet Service Provider broadband connection from the Internet.
Transportation Business Units	The MDOT Transportation Business Units are defined as MDOT HQ (TSO), MAA, MDTA, MPA, MTA, MVA, SHA
MDOT	All TBUs (MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA) within the organizational structure of the MD Dept. of Transportation.
User's Supervisor	The User's Organizational Group Supervisor

IT COTR (Information Technology Contracting Officers' Technical Representative)	The IT COTR for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
Remote Access Administrator	The individual(s) designated as the Remote Access Administrator(s) for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
NOC	The MDOT Network Operations Center (NOC).
INFOSEC	The Information Security group within MDOT and its contractor

3.6.1 MDOT Remote Access Categories

Remote Access – Network Connection

This refers to remote access to the MDOT and TBU network that provides a direct connection to the network. This access requires two-factor authentication.

Remote Access – Service Access

This refers to remote access to the MDOT and TBU services and applications contained on the internal network. This access is offered through SSL connection via the MDOT Secure Portal (a form of secure reverse proxy)

Section 4: Password Policy

4.1 Purpose

The purpose of this policy is to insure when choosing a password, that it is extremely difficult for a potential intruder to make educated guesses about the selected password. This leaves the intruder no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a computer trying one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. In the event of a conflict between State, MDOT or TBU policy, the most stringent shall apply.

4.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, as well as any individual using MDOT resources. This policy applies to passwords required for all network and computer systems. Any device that requires an exception to this policy must be submitted and approved by the SWG.

4.3 Policy Statement

User accounts are provided for the purpose of conducting the business of this Agency and supporting the mission of each department. Computers and networks provide access to local and remote resources, as well as the ability to communicate with other users worldwide. Such open access is a privilege requiring individuals to act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

4.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement the policy. Each staff member with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

4.5 Guidance

The following are general password policies applicable for most systems and must be implemented if the system (operating system or software application) supports it:

Passwords and User IDs are unique to each authorized user.

Passwords for users-consist of a minimum of 8 alphanumeric characters (no common names or phrases). There shall be computer-controlled lists of prescribed password rules. Periodic testing to identify any password weaknesses (e.g., letter and number sequences, character repetition, initials, common words, and standard names) must be performed at least on a yearly basis where applicable.

The root or administrator account has a minimum password length of 11 characters.

Passwords are not the same as the User ID.

Passwords must not consist of all numbers, all special characters, or all alphabetic characters.

Users, Root and Administrators have at least one non-letter character in their password.

Passwords are changed every 45 days for users and every 30 days for system administrators. Most systems can enforce password change with an automatic expiration and prevent repeated or reused passwords.

Password history does not allow users to reuse any password in his/her last 10 attempts.

User accounts disabled after 4 consecutive failed login attempts.

Sessions suspended or locked by means such as a password-protected screensaver after 15 minutes of inactivity and require the password to be reentered to resume the session.

User accounts are disabled after 60 days of inactivity and deleted after 90 days of inactivity unless exempted by the TBU COTR or a manager of the TBU COTR.

User accounts are removed or disabled within 72 hours after notice to the TBU COTR that there has been termination of employment of the user.

Where applicable, successful logons should display the date and time of the last logon and logoff.

Users not allowed to use common passwords and passwords must not be based on personal information, i.e. username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.

Passwords are kept private i.e., not shared, coded into programs, or written down.

When an employee has a change in job duties and no longer needs access to a system, the account will be removed immediately.

4.5.1 Acceptable Use

Computers and networks are provided for the purpose of conducting the business of this Agency and to support the mission of each department. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with federal, state or local government personnel, vendors and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State association, government advisory or standard activities;
- Communications for administrative purposes
- Group or shared ids are prohibited unless they are documented as Steady State Accounts or Functional ID's. Steady State Accounts, Functional ID's are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., ACF2 id used to run production jobs). Passwords associated with functional ids are exempt from the password sharing and change requirements specified above

4.5.2 Restrictions

MDOT services may not be used for unlawful activities, commercial purposes not under the auspices of this Agency, personal financial gain, or personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines.

4.5.3 Representation

Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the MDOT or State

4.5.4 Interference

Services provided to MDOT shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or solicited interference with others' use of the systems provided

4.5.5 No Expectation of Privacy

Privacy of services such as email is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by MDOT. The State affords electronic mail privacy protections comparable to that which it traditionally afforded paper mail and telephone communications within the context of the State's legal and other obligations.

4.5.6 Security

Password security is the complete and sole responsibility of each individual. Users must take all reasonable precautions to prevent the use of the account by unauthorized individuals.

No user will be required to disclose his or her password.

Systems may be reviewed on a periodic basis to ensure the password policy compliance is being enforced.

4.5.7 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Section 5: External &Third-Party Networks Policy

5.1 Purpose

The purpose of this policy is to describe the "permitted uses", connection methods, and security controls for external (public) and remote, Third Party Networks connecting to the Maryland Department of Transportation (MDOT) network and devices.

The MDOT network allows access from the public to connect to their public servers that are located in the DMZ or service network. The DMZ (demilitarized zone) is a section of the network that resides between the public (untrusted) and the internal (trusted) network. Publicly accessible servers such as Web servers and FTP servers reside in the DMZ.

Third Party Networks are defined as networks that are not part of MDOT, or their network address space, requiring remote connectivity and access to devices within the MDOT Network. This policy also applies to Virtual Private Network (VPN) connections from MDOT to a Third-Party Network for accessing resources on their network. This policy requires that all Third Party Network connections will require the submission of a Remote Access Form as defined the in the guidance of Section 4, Remote Access Policy of the MDOT Security Plan. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

5.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, and to any individual using MDOT resources. This policy applies to all agencies and organizations connecting to the MDOT network.

5.3 Policy Statement

Network services are provided for the purpose of conducting the business of this Department and supporting the mission of each Transportation Business Unit (TBU). Computers and networks provide access to local and remote resources as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individuals act responsibly and observe all relevant laws, regulations and contractual obligations. All Third Party or External Networks are considered or assumed to be un-trusted and are subject to review and compliance with the requirements specified in this policy.

5.4 Responsibilities

Each TBU is responsible for developing policy that is entirely consistent with this MDOT policy, or adopting this policy as the TBU policy. The unique needs of each TBU's business

and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

5.5 Guidance

In strictly controlled situations, MDOT will allow Third Parties to access MDOT internal networks and computer systems. Both the owner of the MDOT information to which the Third Party will be granted access and the Third Party's Management Representative, must agree in writing, to such access before it is established. The Management Representative from the Third Party is also obligated to sign the MDOT Network Connection Terms and Conditions for Third Party Network Access" disclaimer (Appendix C). The decision-making process for granting such access includes consideration of the controls on the systems to be connected, the Third Party's security policies, and a network diagram of the relevant network segment(s) that will be connected to MDOT. The diagram, to be provided by the Third Party or developed internally must include the IP addresses, protocols, and equipment relevant to the connection.

MDOT will terminate the connection of Third Party network to the MDOT network at the conclusion or termination of a contract or project or at any such time that the connection is no longer required. With the approval of the Department CIO, MDOT reserves the right to terminate any connection in which a security breach is believed to be occurring or has occurred and corrective action has not been taken that meets the requirements of MDOT.

5.5.1 Acceptable Use

All network traffic passed from external networks must pass through an MDOT firewall. The following methods are accepted for permitting traffic from the public or Third-Party networks to MDOT's network:

Private leased line: A private leased line (e.g., frame relay, CCT1, TLS, etc.) can be connected from a Third-Party network to the MDOT vendor service network. The Third-Party network will be responsible for purchasing and providing the leased line service to include the circuit and associated hardware (routers, CSU/DSUs, cables, etc.) to establish the connection outside the MDOT network. Third Party responsibilities shall also include installation, maintenance, and problem solving of the network circuit and hardware. Network devices are preferred to be rack mountable. Device must be SNMPv2 manageable. Third Party is requested to provide MDOT, at a minimum, a read-only SNMPv2 Community String to permit device monitoring (CPU, memory, interfaces, etc.) by the MDOT Network Operation Center (NOC) network management tools. MDOT personnel are responsible for implementing the appropriate changes to the MDOT router(s) and MDOT firewall configuration to allow the traffic from the Third-

Party network to the entities within the MDOT network that is needed. Any data being passed through a private leased line that is deemed sensitive or critical must be encrypted. MDOT provides no security management of Third Parties connecting to this shared vendor service network. Vendors should provide their own security of that connection.

Internet from Third Party Networks: Any traffic being passed from the Third-Party network to MDOT using the Internet requires encryption. MDOT will require a Virtual Private Network (VPN) tunnel to be established from the Third-Party network to the MDOT enterprise firewall or to a VPN device/product used exclusively for that system approved by MDOT. The VPN must be established in one of the following methods: (a) firewall-to-firewall, (b) approved VPN client software to MDOT firewall, or (c) approved router to MDOT firewall. The VPN must employ IPSEC encapsulation; AES-256 encryption (Advanced Encryption Standard) and SHA5 hashing algorithm are required unless otherwise approved by the MDOT Security Working Group.

5.5.2 Internet from the public

All access from the general public to MDOT public servers must be terminated at the DMZ. The firewall must be configured to direct all traffic (including http/https) from the general public or from Third Party Networks only to the DMZ, creating a separation of the DMZ from the internal network. Any Web server in the DMZ that accepts or processes credit card payments are subject to PCI compliancy restrictions.

Network access granted by MDOT to the Third-Party network is restricted to only the hosts, protocols, and ports that are needed by the Third Party network in order to support their project or contract requirements. The Third-Party network is responsible for providing MDOT with this information in writing. All configuration changes made to MDOT network hardware or software are subject to review and approval of the MDOT Change Advisory Board (CAB). The MDOT CAB meets weekly to review and approve/disapprove network configuration updates.

Access granted from the public to servers in the MDOT DMZ are restricted to only the hosts and basic protocols that are required. All configuration changes needed for access from the public to the DMZ are subject to the review and approval for the MDOT CAB. Public servers in the DMZ are assigned a public IP address registered to MDOT which is translated to a private IP address assigned for the MDOT DMZ.

5.5.3 Acceptable and Prohibited Cryptographic Protocols and Cipher Suites

Cryptographic protocols are protocols that are designed to provide and assure secure communications offering privacy and encryption of data. The combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms that are used to negotiate the security settings for the cryptographic protocol is called a *cipher suite*. Over the course of time, protocols and cipher suites are

strengthened as hacking becomes sophisticated, thus older protocols are no longer recommended and supported. MDOT follows this paradigm to assure that a low risk factor exists in our network.

The following cryptographic protocols are not permitted in MDOT:

SSLv2, SSLv3, SSHv1

The TLSv1 cryptographic protocol is currently allowed but not preferred by MDOT. The following cryptographic protocols are permitted in MDOT:

TLS1.1, TLS1.2

The following weak cipher suites are not permitted in MDOT:

RC4, MD4, MD5, export-grade cipher suites

5.5.4 Representation

Third Parties shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT, TBU, or any unit of the State unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing MDOT or the State.

5.5.5 Interference

Services provided to MDOT and its TBUs shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive demand on any network resource or computing facilities, or unwarranted or unsolicited interference with others' use of the systems provided.

5.5.6 No Expectation of Privacy

Privacy of services and communications, such as email, is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by this Agency. The State does afford electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations.

5.5.7 Security

As a condition of access to MDOT's computer network, every Third-Party network must secure its own connected systems in a manner consistent with MDOT's requirements. MDOT reserves the right to immediately suspend network connections with Third Party systems not meeting such requirements or if security concerns arise, until those requirements are met.

All Third Party external network connections will be brought before the MDOT Security Working Group for review and approval. MDOT reserves the right to perform a network vulnerability assessment (scan) of any mission critical hosts on the Third-Party network after providing prior written notification of MDOT's intent to do so and specify a time range during which the scan will occur.

Routing of any private Internet Protocol addresses is prohibited. A private IP address is defined in RFC 1918, in which the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Public IP addresses are defined as those that have been legally registered through the InterNIC. MDOT will not route their registered IP addresses assigned to internal hosts over the Internet.

5.5.8 Records Retention

State Records must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Records communicated via Email are disposed of within the record keeping system in which they have been filed in accordance with [the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records.

Section 6: Kiosks Security Standards

The following standards should be followed whenever possible and if the facility can accommodate them.

6.1 Operating System Security

A. Password Protect the BIOS (8-character minimum, (larger when possible).

B. Operating System should the latest possible release of Windows whenever possible.

C. Operating System should auto-logon with a user account that has a password that adheres to the MDOT Security Policy for password complexity

D. The Administrator account should be renamed.

E. Block Internet access[3], assign a static IP address to Kiosk and remove DNS.

F. Create a Kiosk user profile and augment with policy editor.

1. Remove Run command from Start menu.
2. Remove folders from Settings on Start menu.
3. Remove Taskbar from Settings on Start menu.
4. Remove Find command from Start menu.
5. Hide drives on My Computer
6. Hide Network Neighborhood
7. Hide all items on Desktop
8. Disable Shutdown Command
9. Disable Registry Editing Tools

6.2 Physical Security

A. Configure switch port to only accept MAC address of Kiosk PC.

B. Bolt Kiosk in place.

C. Secure Kiosk access panels with commercial grade lock.

[3] When business reasons call for internet access, the MDOT Change Process will be followed to assure the necessary mitigation takes place.

D. Network cable should be placed in a conduit (ex. Greenfield) if the cable can't be run through the floor under the Kiosk.

E. Network cable should be permanently attached to the jack or encased in a strong locked cover if it is accessible.

F. Request the Kiosk to be placed in view of a security camera.

G. A physical site assessment must be performed by the MDOT Information Security team before the kiosk is approved for production and public accessibility. This must be noted in the Maximo Service Request. A letter stating the customer's knowledge of the visit and an attempt being made to challenge existing security procedures will be provided to the INFOSEC team doing the visit and signed by the customer.

Sample Customer Acknowledgement Letter.

October 09, 2013

To Whom It May Concern:

The MDOT (insert TBU name) has engaged personnel listed below to perform a vulnerability assessment and analysis beginning on MM/DD/YYYY and completing on MM/DD/YYYY. In the process of conducting this authorized exercise, the authorized personnel will ignore or challenge existing TBU and MDOT system security procedures as necessary to ensure that an effective assessment is performed. To verify the validity of this letter and authorized personnel, please check with the primary contact listed for the facility. If the primary contact cannot be located, please call [applicable client personnel and telephone number(s)] for verification.

This assessment is being performed at (list locations and/or list of network addresses)

AUTHORIZED PERSONNEL

NAME
NAME

LOCATION (S)	**PRIMARY CONTACT (S)**
As Applicable	As Applicable

Thank you for your cooperation.

Signature

Name of Client Authorized Manager

Title /Position
Telephone Number
Address

Section 7: Internet Web Hosting Policy

7.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to the Internet and provide public information access. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

7.2 Scope

This policy applies to all Internet Web server systems that are being built or in working condition regardless of whether they are hosted within MDOT or by a Third Party. Close attention should be made not only to the Web server itself, but also the security needs and requirements of the local network and other interconnected networks. In the case of collaborative efforts between MDOT and another governmental entity, MDOT management shall exercise due diligence to ensure that the intent of this policy is adhered to by the hosting party.

7.3 Policy Statement

There are many areas of Web servers to secure such as the underlying operating system, the Web server software, server scripts, and other associated components. All Agency Web servers that are accessible from the Internet must adhere to the following standards for operation and maintenance:

7.3.1 MDOT Hosting Policy:

1. Information placed on any Web site is subject to the same privacy restrictions as releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information.

2. A public Web server must not serve as a repository for confidential data, although it can act as a proxy for access to confidential data located on more secure hosts.

3. Users are forbidden to download, install or run Web server software without prior approval by the user's Agency authorized system administrator.

4. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

5. Web server software and the underlying operating system must employ all security patches and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

6. Place Web servers on subnets separate from internal networks.

7. Firewalls and routers must be in place and configured to restrict attacks from public and internal networks as well. Only traffic needed for browsing and business applications management is allowed through the firewall to access that server.

8. Since using a computer simultaneously as a public Web server and for other public Web services poses risks, a computer must be dedicated to the sole function as a Web Server. Specifically, business or personal files are vulnerable to a malicious Web user if access is gained to a directory on your computer.

9. Keep the computer free of any networked or shared drives to another system. Access to remote machines opens an avenue for a malicious user to breach security.

10. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users. Ensure MDOT password policy is followed.

11. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. A review of logs on a regular basis by authorized personnel to record and report anomalies to your organization's designated security point of contact is desirable.

12. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place.

13. An MDOT-approved Third Party will perform Web server security assessments bi-monthly unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes (not page content), etc. The Modal COTR and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

7.3.2 Third Party Hosting Policy:

MDOT hosting policies in sub-paragraphs 1, 2, 5, 7, 9, and 10 of paragraph 9.3.1 above also apply to Third Party Hosts. In addition, the following policies also apply:

1. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place. The Third-Party Host must be able to take off-line any portion of the Website that has been compromised.

2. The State will contract a Third Party to perform Web server security assessments after the initial assessment, at the discretion of MDOT, unless unforeseen events require immediate assessment. The Third-Party Host will provide written authorization for MDOT to perform these security assessments as part of the original contract. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal COTR, IT Manager and Third-Party Host will be informed before the assessment is done and receive a copy of the results.

3. Non-compliance with policy directives may result in revocation of the Web Hosting contract. Additionally, MDOT content will be removed from the server and MDOT will retain the rights to the domain name.

7.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

7.5 Guidance

This section establishes "high level" guidelines and standards supporting the agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

7.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

7.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 8: Intranet Web Hosting Policy

8.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to an Intranet. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of the Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

8.2 Scope

This policy applies to all Intranet Web server systems that are being built or in working condition regardless of whether they are hosted within the MDOT or by a Third Party. Close attention is required for the Web server as well as the security needs and requirements of the Intranet since they frequently house sensitive corporate information not intended to be viewed by anyone outside the Agency. Intranets clearly illustrate how challenges to security are not so much technical as they are procedural.

8.3 Policy Statement

There are many areas of Web servers to secure including the underlying operating system, the server software, server scripts, and other associated components. Noteworthy, Intranets require strict internal security policies and procedures to control access to sensitive corporate data from within. Even though Intranet Web servers are not accessible from the Internet, they remain susceptible to the same attacks including penetrations from the Internet via other systems on the "inside network", and also through Internet Web browsing from the server. All Agency Web servers must adhere to the following standards for operation and maintenance:

1. Information placed on any site is subject to the same privacy restrictions when releasing non-electronic information. Accordingly, before information is place on the Intranet, it must be reviewed and approved for release in the same manner as other official memos, reports or other official non-electronic information.

2. Users must not run Web server software without prior approval by a user's Agency-authorized System Administrator.

3. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

4. Server software and the underlying operating system must employ all security patches no later than one month of release and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

5. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users.

6. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. Additionally, authorized personnel must review logs regularly to record and report anomalies to your organization's designated Security Officer.

7. Procedures for Web Server users to report any dramatically unexpected changes on the site to system administrators or your organization's designated Security Officer must be in place.

8. A Third Party will perform Web server security assessments annually unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

8.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

8.5 Guidance

This section establishes "high level" guidelines and standards supporting the Agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

8.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

8.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed

and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 9: Wireless Communication Policy

9.1 Purpose

The purpose of this document is to define a policy for securing wireless connections within MDOT's network. Due to the inherently insecure nature of this technology, only secure wireless systems that meet the requirements in this policy are approved for connection to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

9.2 Scope

This policy applies to all MDOT employees, and staff subordinate to MDOT contracts. It is recommended that the "Policy Statement" be included in any contract award process. This policy covers all wireless networking devices (e.g., Wireless Access Points, bridges, computing devices, etc.) connected to any of MDOT's internal networks. Wireless devices and/or networks without any connectivity to MDOT's networks do not fall under the purview of this policy.

9.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. The security and integrity of this network must be upheld when utilizing wireless networking devices on the MDOT network.

In keeping with State of Maryland Department of Information Technology (DoIT) policy (Version 2.2) regarding Wireless (section 7.8), the following guidance will be observed:

- Establish a process for documenting all wireless access points
- Ensure proper security mechanisms are in place to prevent the theft, alteration. Or misuse of access points
- Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available
- Change default administrator credentials
- Change default SNMP strings if used, otherwise disable SNMP
- Change default SSID
- Deploy secure access point management protocols and disable telnet
- Strategically place and configure access points so that the SSID broadcast range does not exceed the physical perimeter of the building (unless the wireless solution is designed for providing outside connectivity).
- Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services

- Require wireless users to utilize encrypted data transmission if accessing internal LAN services

This MDOT/MDTA Wireless Communication Policy provides this additional guidance:

- No wireless access points shall be connected to the MDOT network without following the MDOT Change Management process.
- No end user device connected to the MDOT network (either wired or wireless) shall offer or allow connections to or from other networks
- No end user device will broadcast MDOT SSIDs or otherwise masquerade as a device providing connections to the MDOT network
- No MDOT wireless network management interfaces shall be accessible from the wireless network
- Wireless networks providing access to internal MDOT resources require WPA2 (Wi-Fi Protected Access - Enterprise) with two factor authentication.
- Wireless networks providing guest access to the Internet shall implement WEP (Wired Equivalent Privacy) at a minimum.
- Guest wireless network accounts will be unique and will be configured to expire passwords after eight hours. Exceptions to this policy must follow the MDOT Change Management process. For example, a one-week training class requiring guest wireless access may require an exception to the policy.

9.4 Responsibilities

Each Agency is responsible for developing procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

9.5 Guidance

All wireless networking devices providing a wired connection to the MDOT network must have approval from the Security Working Group and be submitted for review via the Change Management process prior to being connected to the MDOT network. Due to the highly evolving nature of this technology, an MDOT Wireless Standards document (see Appendix D) will be kept on an on-going basis that contains current MDOT implementations of these technologies, known issues, and recommendations.

Wireless devices found to be non-compliant with this or other appropriate policies (ie. Remote Access Policy, Email and Internet Use Policy) will have their connection terminated **immediately**.

Section 10: Secure FTP Policy

10.1 Purpose

The purpose of this policy is to support the appropriate use of secure and non-secure FTP access privileges for both MDOT and external users. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT/MDTA without the expressed written permission of the MDOT CIO.

10.2 Scope

This policy applies to an individual, government agency, or business-trading partner who has been given authorization to access the Maryland Department of Transportation (MDOT) Secure FTP Server from a remote site. This policy applies to all MDOT/MDTA Modal Agencies operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy will follow a structured review and approval process.

10.3 Terminology

The following table defines terms used to describe various devices, entities and groups within this document:

The Network or Enterprise Network	The combined MDOT Network and associated MDTA Network components.
Secure FTP Server	Private transfer file transfer system offering enterprise grade security.
MDOT	Maryland Department of Transportation
MDTA	Maryland Transportation Authority
NOC	Maryland Department of Transportation Headquarters
CCB	Configuration Control Board
CIO	Chief Information Officer
CCR	Configuration Change Request
DPPA	Driver's Privacy Protection Act
FTP	File Transfer Protocol

RDA	Records Disposition Authorization
SARA	State Archives and Records Administration

10.4 Policy Statement

Secure FTP access is made available for users and entities that are responsible for policy review, approval, implementation, enforcement, as well as equipment procurement and maintenance. Computers and networks provide access to remote resources, as well as the ability to communicate with other users worldwide. Open access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations.

MDOT HQ and the Configuration Advisory Board (CAB) are responsible for approving; implementing and enforcing the MDOT/MDTA Secure FTP Access Policy. The request is submitted to the Security Working Group for discussion and review. If agreed upon, the request is presented to the CAB. When accepted by the CAB, the request is presented to the IT Modal managers and, upon approval, is incorporated into this policy.

Secure FTP Access Policy is developed by the MDOT HQ sanctioned Security Working Group and submitted to MDOT CIO and the corresponding CCB for interim approval. The MDOT CIO will present the proposed policy to the IT Modal Managers/IT Teams for final review and approval.

Approved Secure FTP access Policy is implemented under the direction of the MDOT HQ and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

10.5 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The following sections define the Secure FTP Access responsibilities of the individuals listed below:

- Secure FTP access User
- System Administrator
- Secure FTP Access Administrator
- NOC Help Desk

10.5.1 Secure FTP Access User

Secure FTP Access Users are defined as business trading partners who require secure FTP access to the MDOT/MDTA Secure FTP Server.

If required, the Secure FTP user is responsible for obtaining the Request Form from the prospective MDOT/MDTA Modal Agency, completing and signing the first section of the Secure FTP access Request Form, and forwarding it to the Agency's Project Coordinator. Modal Agencies may assign this responsibility to their Project Coordinators.

The Secure FTP Access User is responsible for reporting Secure FTP access Client or Application Software problems to the appropriate Help Desk.

The Secure FTP access User is responsible for all system hardware and software maintenance to their personal computer. MDOT and MDTA are not responsible for the condition of the secure FTP access User's personal computer.

10.5.2 System Administrator

The Agency's System Administrator is responsible for reviewing the Secure FTP Access Request Form to ensure that the user has completed and signed the portion of the form designated for the user.

The System Administrator authorizes the request by signing the FTP Access Request Form and specifying the types of access the User will be granted. The Secure FTP Access Administrator who updates access controls processes the form.

10.5.3 Secure FTP Access Administrator

The Secure FTP Access Administrator is responsible for the following:

- Coordinating activities associated with the Secure FTP access Request Form. He/she ensures the information on the form is correct and signed by both the user and the Agency's System Administrator.
- Providing the NOC Help Desk with the information required in creating Secure FTP access directories. In this case, the Secure FTP Access Administrator faxes a copy of the Secure FTP access Request Form to the NOC Help Desk.
- Providing the User with passwords, configuration information, installation software, and manuals, required to access the Secure FTP Server remotely.
- Providing training to the Agency's Project Coordinator on the use of applications required for Secure FTP access, if required.
- Maintaining a file containing the signed copies of the Secure FTP Access Forms.
- Notifying the Agencies Project Coordinator when the account is setup.

10.6 NOC Help Desk

The NOC will provide priority level "Critical" support for Secure FTP Server specific problems as contractually agreed to with MDOT.

10.7 Guidance

A User wanting to access the MDOT Secure FTP Server must obtain authorization from the prospective MDOT Modal Agency. The User can obtain the Secure FTP Access Request Process from the Agencies FTP Access Administrator.

The Secure FTP client should complete, sign and return the following documents, if required by the Modal FTP Administrator:

- The Agency's FTP Driver's Privacy Protection Act (DPPA) compliance contract, which outlines the Users responsibilities under the Federal DPPA.
- Third Party External Communications Network Security Policy and MDOT Network Connection Terms and conditions for Third Party networks.
- The Agency's FTP Access Request Form.

Upon receipt and approval of the signed Secure FTP Documents, each Modal will transmit in a responsible and secure process, the Account User ID and password to either internal or external Users depending upon the location of the User. After the User signs on and modifies the default password, he/she should perform a verification test. Directions will be provided on whom to contact for lockouts of User ID and passwords if applicable.

10.8 Acceptable Use

Access to Secure FTP is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards;
- Communications for administrative purposes.

10.9 Restrictions

Secure FTP access may not be used for unlawful activities, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Secure FTP access:

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

- Transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;

- Use for any purpose that is against State or Public policy or contrary to the State's best interest;

- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;

- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

- Misrepresenting in any manner, your identity, your account or a computer in electronic communication;

- Knowingly sharing a personal account;

- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;

- Unauthorized Disclosure of confidential or proprietary information.

10.10 Representation

Secure FTP Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

10.11 Interference

Secure FTP access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Secure FTP access systems. Such uses include, but are not limited to chain letters, "Spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

10.12 No Expectation of Privacy

Privacy of Secure FTP Access is not guaranteed. Authorized State Employees may access and disclose the contents of all messages created, sent or received using the MDOT/MDTA Secure MDOT/MDTA Secure FTP Server.

10.13 Security

The following specific guidance relating to Secure FTP access security is provided:

- **Encryption**

All external users connecting to the Secure FTP server will use a minimum of 128-bit encryption. The server will only allow connections with 128-bit encryption or better if originating from an external network.

- **Disclaimer**

Modal Secure FTP Access Users are defined as Government Agencies or Businesses who require secure FTP access to the MDOT Server. Access to the MDOT Secure FTP server is considered a privilege.

MDOT assumes no responsibility for any hardware, operating system, or software application problems encountered by any MDOT Modal Secure FTP Access User when installing/using the designated security applications to connect to the MDOT Secure FTP Server.

10.14 Records Retention

Files transferred using Secure FTP access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Files

needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Secure FTP access system in accordance with each Department's standard practices.

Records transferred via Secure FTP access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

10.15 Secure FTP Access Administrators

Each Modal /Agency will assign their own Secure FTP Access Administrator.

Section 11: Vulnerability Assessment Scan Policy

11. 1 Vulnerability Assessment Scanning

11.1.1 Responsibilities

The Office of Transportation Technology Services (OTTS) IT Security office or the network managed services (NMS) contractor will perform server vulnerability assessment (VA) scans on a regular basis (scheduled or on request) unless unforeseen events require immediate assessment. Also, security assessments scans must be initiated after major application configuration changes. The Transportation Business Unit (TBU) Contracting Officers' Technical Representative (COTR) and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

11.1.2 Types of Scans

A *vulnerability assessment scan* is defined as a systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

A *discovery scan* runs on MDOT's subnets detecting all IP based hosts. Ports are scanned and services associated with those ports are enumerated. No vulnerabilities are determined during these scans.

A special Web server scan is run for Web servers that are located on the DMZ or internal MDOT network. This scan will crawl or spider each Web page, following all the links, perform code analysis, and perform vulnerability detection.

11.2 Frequency of VA scans

11.2.1 Pre-Production On Demand VA Scans

All new servers that are being placed in a production environment must pass a vulnerability assessment (VA) scan. The initial VA scans are performed by the server administrator/TBU management after the operating system is installed and ready for the test and development environment. This will give them the opportunity to remediate any vulnerabilities that are reported before submitting the request for the final scan to the OTTS IT Security or NMS contractor for the final scan. The final scan is performed by OTTS IT Security or NMS contractor personnel after the server is configured and the developer installs the application code onto the server, readying it for the production environment.

Additionally, assessments must be performed after major configuration changes deemed appropriate during the Security Review of the Change Request approval process.

11.2.2 Ongoing/Monthly Scheduled Scans

Vulnerability assessment scans of each TBU are run monthly. This consists of scanning all TBU resources including servers and workstations. During the scan, ports are scanned and services are enumerated. Based on the operating system, the assessment may require to login into the system or application, which requires credentials that are provided by the server administrator to be in place for the scan. All of the data gathered is processed through a very extensive matrix to determine vulnerabilities with remediation recommendations.

Discovery scans are also run ongoing throughout the network.

11.3 Criteria

The OTTS Office of IT Security or NMS contractor will determine based on the results of the scan whether the server passes or requires remediation. A risk score is provided in the report. Judgment is made on the severity of the vulnerability and the risk that it poses to the integrity of the MDOT network (likelihood of attack or exploitation).

The server administrator is expected to mitigate any of the vulnerabilities those are deemed to pose a high risk to the MDOT network. After remediation, another scan will be run to determine if the risk still exist. In cases where the server administrator/TBU management cannot remediate the vulnerability but requires placement of the server in the network, they must accept the risk and initiate a Safeguard Implementation Plan (SIP, Section 16) with the OTTS Office of IT Security.

11.4 Scans from Third Party Vendors

Any Web server that process or stores credit card data for online electronic transactions are subject to a scan to meet Payment Card Industry Data Security Standards (PCI DSS) requirements. The PCI scan must be performed by an external (Third-Party) Approved Scanning Vendor (APS). The TBU IT leads must arrange these scans with the OTTS Office of IT Security or NMS contractor, and make sure that the scheduled task is on the NOC calendar. A Service Request/Change Request must be opened if the scan requires temporary firewall changes to allow the scan to take place.

Any server(s) for which a TBU's business system or application is resident on that is hosted by a Third Party outside of the MDOT network must have a VA scan run quarterly by the Third-Party vendor. The vendor is responsible for providing the scan report to the TBU COTR and the OTTS Office of IT Security. The vendor is responsible for remediating any high or critical risk vulnerability under the direction of the OTTS Office of IT Security.

11.5 Communication of New Vulnerabilities

As new vulnerabilities are discovered or announced, the MDOT NMS InfoSec contractor or OTTS Security Team shall inform each COTR via email with a description of the vulnerability,

it's risk to the MDOT environment and where possible and practical, a means to mitigate or protect the TBU from the risk that the vulnerability presents. Sources of such vulnerability information include but are not limited to:

MS-ISAC

US-CERT

Vendor sites such as Cisco, Adobe, etc.

SANS Institute

Section 12: Computer and Network Equipment Disposal Policy

12.1 Purpose

The purpose of this policy is to describe the permitted disposal methods for devices that may contain data storage either on hard disk, removable media, or within memory. This includes, but is not limited to, computers, servers, routers, switches, copiers, printers, faxes, multipurpose devices, cameras, and other related equipment. Data left on hard drives, Random Access Memory (RAM), Flash Memory or Non-Volatile Memory can contain proprietary information or data that is sensitive to the security of the network and MDOT information. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

12.2 Scope

This policy applies to all MDOT and MDOT Transportation Business Units (TBUs) employees, and personnel subordinate to MDOT and TBU contracts. This applies to all network and stand-alone computer systems (desktops, workstations, laptops, and servers), routers, switches, hubs, concentrators, firewalls or other network related items. It also applies to systems not located within MDOT that are provided as a service to MDOT. Policy Statement

12.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. Proprietary and/or sensitive data may be permanently stored or cached on the hard drive, RAM, Flash Memory, or Non-Volatile Memory. Proper disposal of this data is required to protect the confidentiality of data and to ensure security of the network.

12.4 Responsibilities

Each Transportation Business Unit (TBU) is responsible for developing an expanded procedure that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT and State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

The MDOT CIO requires that each TBU send a report to the MDOT CIO Office that indicates specific information about equipment that has had to be "sanitized" prior to disposal. That information can be found on the MDOT NOC Portal under equipment sanitization reporting procedure.

12.5 Guidance

Once Computer and/or Network Equipment has been identified as "Excess for Disposal" the equipment will be advertised to all MDOT TBU for five (5) business days to determine if there is interest in acquiring the equipment. Any equipment that is to be reused by a TBU must have the hard drive wiped and reimaged. Any equipment not requested by a TBU will be disposed of as mandated in DGS' Inventory Standards & Support Services Division (ISSSD) Inventory Control Manual.

As stated in Section 6.4 of the Department of Information Technology's (DoIT's) Information **Security Policy Version 3.1; "**To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. The removed hard drives may either be sanitized with a disk wiping utility and re-used within an agency or must be physically destroyed such that they are permanently rendered functionally useless. Agency CIOs will be responsible for the hard drive removal, recycling, destruction and/or disposal process.

A request for waiver is to be submitted to DoIT's Enterprise Information Services for authorization of disposal of a device with a hard drive and/or electronic memory with justifying documentation to support that the media has been overwritten in accordance with U.S. Department of Defense media sanitization standards.

As stated in Section 6.5 of the Department of Information Technology's (DoIT) Information Security Policy version 3.1, "To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. Note: Disposal of electronic storage media should be in compliance with the agency's document retention policy and litigation hold procedures. Additionally, the procedures performed to sanitize electronic media should be documented and retained for audit verification purposes. This policy applies to all electronic storage media equipment that is owned or leased by the State (including, but not limited to: workstations, servers, laptops, cell phones and Multi-Function Printers/Copiers)."

Additional guidance will be provided using NIST Special Publication 800-88 Table A-1 Media Sanitization decision matrix.

Section 13: Network Access Policy

13.1 Purpose

The purpose of this policy is to describe the criteria a computer system must meet before being able to connect to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. Scope

This policy applies to anyone that needs to connect a microcomputer or server to the MDOT network including, but not limited to all MDOT employees, staff subordinate to MDOT contracts, and visitors. This applies to all computer systems (desktops, workstations, laptops, and servers) that need access to the MDOT network.

13.2 Policy Statement

Computers and networks provide access to MDOT and resources, as well as the ability to communicate with other users worldwide. All systems must be secure and up to MDOT standards before they will be allowed access to the network.

13.3 Responsibilities

Each Agency is responsible for developing policy and/or procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

13.4 Guidance

All computer systems must meet MDOT standards before access will be allowed on the MDOT network. MDOT has a policy of disabling unused network ports. The Modal Help Desk should be contacted to request access to the MDOT network and a Help Desk ticket will be created to ensure compliance with this policy. If currently disabled, the port will be activated within 24 hours of contacting the Help Desk. The following standards must be met before connection to the MDOT network is allowed.

- **Operating system patches up to date**

  Any microcomputer system and server must be up to date with the latest security patches for the operating system. The server administrator must apply all of the latest security patches and updates within a month after the updates are announced or immediately if the update is critical.

- **MDOT/MDTA has an account with administrative rights to the system**

Any microcomputer system and server that will be directly connected to the MDOT network longer than one day must have an MDOT account with administrative rights to the system accessible by the Modal technical staff. Any exceptions to this must be granted by the MDOT CIO in writing.

- **Antivirus Protection**

  Antivirus protection must be installed on the microcomputer system or server. The software must be configured to run at startup and stay memory-resident to check for viruses during normal activity. The software must also be up to date with the latest virus signatures.

If new and/or third-party systems (including laptops) need to be connected to the network in order to be patched, updated, or any other reason in order to meet MDOT standards, this activity can be performed by connecting to the secure build areas that are segregated from the MDOT network at the discretion of the Modal. It is the responsibility of the Third Party to update third-party systems.

Section 14: Safeguard Implementation Policy

14.1 Purpose

A. The State of Maryland Department of Transportation (MDOT) recognizes the need to mitigate and ultimately correct risks introduced to the MDOT Enterprise to the extent that it is plausible and possible.

B. MDOT further recognizes that it needs to be able to continue to serve its customers while mitigating or correcting a discovered risk to the enterprise unless the risk is so extreme that it requires immediate resolution to avoid potential loss or disclosure of critical IT Resources, Systems or Data.

C. MDOT requires Safeguard Implementation Plans to assist the organization in managing an identified risk in a controlled and structured manner. These plans contain information on risk details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to the identification of a specific risk(s) to the MDOT Enterprise.

14.2 Scope

A. This policy applies to the Maryland Department of Transportation (MDOT) organizations, their staff, and their contractors that manage and maintain computing devices and data communication devices that connect to the MDOT Enterprise Network.

14.3 Policy Statement

A. The Maryland Department of Transportation Office of Transportation Technology Services (OTTS) shall develop and maintain a Safeguard Implementation Plan (SIP) for any risk that is identified within the MDOT Enterprise[4].

B. The SIP will contain information pertinent to the nature and severity of the risk, a risk level rating, recommended controls, and selected controls for mitigating the risk. Additionally, a projected date for the implementation of each risk migration strategy will be stated and accepted by the parties responsible for the implementation of those strategies.

C. In the event that the risk is determined to be high and the required mitigating strategies cannot be implemented (not technically or financially feasible or cannot be implemented within a one-year period) the SIP documents will be accompanied by a "Management Risk Acceptance Memo" and signed by the Designated Approving Authority for the system in question, the Transportation Business Unit Chief Information Officer, and the MDOT Chief Information Officer.

[4] The Safeguard Implementation Plan shall use the NIST 800-30 Appendix C as a guide for gathering the required information.

D. The SIP and any associated Management Risk Acceptance Memos will be maintained and tracked by the MDOT Office of Transportation Technology Services (OTTS) Office of Data Security (OOS) to assure that the appropriate risk mitigation strategies are put in place in the time frames defined. The MDOT CIO and TBU CIO/Director of IT will be notified of any strategy that is in danger of not being completed or that may require an extension due to unforeseen circumstances.

14.4 Responsibilities

A. The Designated Approving Authority (DAA) is the application or system owner, responsible for assuring that vulnerabilities and associated risks are mitigated to the extent technically and financially feasible, within the milestones defined in the SIP. The DAA must also accept any remaining, or residual, risks associated with the application or system.

B. The Transportation Business Unit (TBU) Chief Information Officer, or his equivalent, shares the responsibilities of the Designated Approving Authority and accepts the risk on behalf of the TBU.

C. The MDOT Chief Information Officer, or his designee, is responsible for accepting risks for the MDOT Enterprise Network and for assuring that Safeguard Implementation Plans are adhered to.

D. The Office of Transportation Technology Services is responsible for coordinating and managing the risk and vulnerability assessment process as well as the creation, management, and monitoring of the SIP and associated documents including the "Authority to Operate" and the "Management Risk Acceptance Memo". This office is also responsible for maintaining this policy and any accompanying procedures.

14.5 Guidance

A. The Safeguard Implementation Plan seeks to follow the guidance provided in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-30 "Risk Management for Information Technology Systems".

14.6 Forms

A. Safeguard Implementation Plan

B. Vulnerability and Risk Assessment with Authority to Operate

C. Risk Acceptance Memo

Section 15: Cloud Computing Policy

15.1 Purpose

The National Institute of Standards and Technology (NIST) defines Cloud Computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.".

15.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) organizations and their staff, that wish to utilize Cloud base services. For the purposes of this policy it is relative to Software as a Service (SAAS), Hardware as a Service and Infrastructure as a service. The scope of this policy is only relevant to publicly available Cloud services, not any MDOT Corporate Cloud services that MDOT may or may not engage in.

15.3 Policy Statement

Cloud computing can offer benefits in the cost, performance, and delivery of information technology services and that the use of cloud computing services will grow significantly over time. This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of information technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Prior to procuring a cloud computing solution, the following issues must be considered in determining the appropriateness:

A. Relevant statutory and policy requirements for the system or data that is being considered, including privacy and personally identifiable information in the data. Resources, State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
B. Records management and retention requirements and the ability to comply under a cloud environment.
C. Procurement and financial implications - there is usually little upfront cost to these solutions but typically a monthly service fee associated with using the cloud solution. Consider the entire life-cycle costs.
D. Issue of interoperability with existing system(s).

15.4 Responsibilities

A. The Initiator of the request is responsible for submitting the Cloud Computing request form and assuring that all appropriate reviews and sign off's have occurred prior to submitting the Service Request. It should be noted that a cloud computing request form must be submitted for each new application or service being considered. Applications negotiated prior to the writing of the policy

B. The Designated IT Authority (DIA) is responsible for assuring that the data to be stored in a cloud based service has been properly classified using the MDOT Standard Data Classification template.

C The Designated Approving Authority (DAA) is responsible for providing the business justification and any cost information associated with using a Cloud based service to perform the business function. They are also the Agency Head or delegated authority for the business giving them the authority to approve the submission of the cloud computing request.

D. The request for using a Cloud based service will be submitted as a Normal Enterprise Change Request (CR) from the Service Request, which is reviewed by the MDOT NMS security, WAN, and systems sections and approved by the MDOT Change Manager. The Cloud Computing request form and the MDOT Standard Data Classification template is attached to the CR.

15.5 Guidance

The MDOT Cloud Computing policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing

Section 16: Mobile Device Access

16.1 Purpose

Mobile access to vital business applications and information empowers workers to be more productive, efficient, and flexible. This enables access to business systems and network resources from mobile devices such as smart phones and tablets. The access is controlled through a Mobile Device Management (MDM) tool to assure confidentiality, integrity, and availability.

16.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) Transportation Business Units (TBUs) and their staff that wish to utilize mobile devices to access the MDOT network. For the purposes of this policy it is relative to the centrally managed MDM suite in regard to granting access to employees and contractors. The mobile devices include smart phones and tablets that are both state-issued and personally owned (Bring Your Own Device or BYOD). Mobile devices that this policy applies to include iOS, Android, and Windows smartphones and tablets

16.3 Policy Statement

Mobile device access offer benefits by enabling MDOT employees and contractors to gain access to the network from their mobile devices, resulting in increased productivity and efficiency. There is also a risk that comes with this convenience, as the features that make smart devices beneficial to employees are also attractive to hackers, data thieves, malware distributors, and other criminals.

This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of Information Technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Mobile device access to the MDOT network is a privilege for authorized users. Users must sign the MDOT Mobile Device Management Acceptable Use Policy found in the appendix prior to being granted the access.

16.4 Guidance

The MDOT Mobile Device Management policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-124 - Guidelines on Managing the Security of Mobile Devices in the Enterprises.

16.5 Device Control

A mobile device serves many purposes, and can have personal and non-work related data stored within it. Also with the use of personally-owned devices (the BYOD concept), there is no assurance that the device is trustworthy. Organizations must assume that all mobile devices are un-trusted until proper measures to secure and monitor the device. The MDM is a technical solution that achieves degrees of trust in BYOD and State-issued devices. It also provides encryption of data in transit and on the device itself.

For personally-owned devices, all MDOT software and data will be maintained in a secure, isolated sandbox/secure container on the mobile device, separated from personal content on the device. This is known as *containerization.* A separate container for MDOT must be present on all mobile devices that are granted access to the MDOT network. This policy only applies to the MDOT container on the device set up by the MDM product, not to the entire device. (Note: for personally owned devices, some wireless carriers charge an extra fee if connecting to another network that passes through an MDM vendor).

For State-owned devices, containerization is not needed. These devices will be fully managed by the MDM and the TBU administrators.

16.6 Authentication Controls

All MDOT employees and contractors that are granted the privilege of using a mobile device to access the MDOT network are set up with a username and password through the MDM system. User accounts must not be shared with other individuals. The following password guidelines in accordance with MDOT and State DoIT are in place for authenticating to mobile devices:

1. New accounts must be set up with a pre-expiring password, forcing the user to create their own password.

2. Passwords must expire every 45 days.

3. The password length must be between 8 and 16 characters.

4. All passwords require an upper and lower-case letter, at least one number and at least one special character.

5. Any device that is idle for 15 minutes will be locked and require the password to be entered to unlock it.

6. User accounts will be disabled after 6 consecutive failed login attempts. Only the MDM administrators can unlock accounts.

16.7 Application Access

Mobile devices afford access to features that may be beneficial for work-related purposes. Some of these features include text messaging, a camera, GPS (Global Positioning System), and other apps. It is at the discretion of the TBU authorizer and MDM administrator to grant access to these features, which are maintained in the MDOT container of the device.

Access to the Internet (Web sites) will pass through the proxy server, enforcing the same controls in place for the employee/contractor working from a desktop. Mobile devices will have access to corporate email within the MDOT container of the device.

16.8 Compliancy Requirements

It is the responsibility of the mobile device user to maintain the most current version of software on their device. Users are responsible for assuring that the latest patches and versions on the device (state-owned or personal) must be present to assure the most sound security practices. This includes:

- The most current version of the MDM software.
- For smartphones, the device must have the most current IOS/Android software.
- Any applications present in the container.
- The MDM will automatically detect if a device has been jailbroken or rooted when logging onto the network. Any device that is detected as jailbroken or rooted will result in the container being erased. *Jailbreaking* is any third-party iPhone application which is installed and not approved by Apple. *Rooting* is unlocking the Android operating system so you can install unapproved (by Google) apps, update the OS, or replace the firmware.

16.9 Device Administration

All MDM administrators will be responsible for assigning the access needed for the users, creating the containers, providing any state-owned devices, and tracking usage. Any mobile device that is lost or stolen must be immediately reported by the user to their MDM administrator. Devices reported as lost or stolen must be wiped immediately.

Section 17: PCI Compliancy

17.1 Purpose

The purpose of this section is to identify all requirements that any TBU has which processes transactions involving credit and debit cards on their hosts in exchange for a service or product that they provide.

17.2 Scope

Any organization or merchant that accepts, transmits, or stores cardholder data (credit/debit cards) must be in compliance with Payment Card Industry Data Security Standards (PCI DSS). While the MDOT IT Security Plan addresses some of the policy subjects that are required for PCI DSS compliance, this section will provide the requirements that are specific for PCI DSS compliancy not addressed elsewhere in this plan.

17.3 Required Scans

Every quarter, any TBU that maintains an external-facing host or hosts that accepts, transmits, or stores cardholder data must undergo and pass a vulnerability scan from an external Approved Scanning Vendor (ASV). This involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network.

A scan must be conducted by an external scan (ASV or qualified personnel) after any significant change to Internet-facing hosts in the DMZ that store, process, or transmit cardholder data. According to PCI DSS requirement 11.2.3, "The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant"

On a quarterly basis, internal vulnerability assessment scans must be conducted on hosts that accepts, transmits, or stores cardholder data, or when a change is made to that host.

17.4 Penetration Tests

On an annual basis, a penetration test must be conducted by qualified personnel on any host that accepts, transmits, or stores cardholder data. Penetration tests must also be conducted after a significant change occurs on any host within scope of PCI (Cardholder Data Environment).

17.5 Wireless Guidelines

The wireless requirements for PCI DSS relate to whether or not the technology is part of the Cardholder Data Environment (CDE). The CDE is the computer environment where cardholder data is processed, transmitted, or stored and any networks or devices that are directly connected

to that environment. In accordance with PCI DSS Requirement 11.1 and 12.9, TBUs must check for and remove unauthorized wireless devices in the CDE on a regular basis, and maintain quarterly reports showing wireless scans of the network that may connect to the CDE which shows that rogue and unauthorized Wireless Access Points (WAPs) being eliminated, or have methodology in place that can detect authorized and unauthorized access points.

17.6 Network Security

In accordance with PCI DSS standard 1.1.6, firewall and/or router configuration for servers that accepts, transmits, or stores cardholder data must be restricted to the secure Internet Protocols of HTTPS (port 443), SSH (port 22) {note – check PCI DSS 3.1 regarding SSH}, or must be passed across a Virtual Private Network (VPN). Firewall and router configuration must be reviewed bi-annually to assure that the CDE is maintained up to standard.

17.7 Encryption

In accordance with PCI DSS standard 4.1, strong cryptography must be present to safeguard sensitive cardholder data over open, public networks. All hosts that accept, process, or store cardholder data must have an SSL certificate from a trusted Certificate Authority (CA) vendor. These hosts must have the Transport Layer Security (TLS) encryption protocol in place {note: review language with TLS}.

17.8 Access and Maintaining Cardholder Data

Access to any cardholder data must be restricted to only those individuals that require it for business purposes. If the Primary Account Number (PAN) is ever displayed, it must be *masked*, meaning that only up to the first six or the last four digits of the account number can be viewed. No individual will have access to data displaying the full PAN without written consent from the TBU's CIO. A designated manager or director from each TBU must maintain a list of individuals that have access to data with the full PAN, their role and business purpose for that access. This list must be reviewed quarterly to determine if any changes are needed.

In accordance with PCI DSS standard 3.4, any TBU that stores cardholder data must have a data retention and disposal policy in place established. Any credit or debit card numbers that are stored must be rendered unreadable if storage is required.

Appendix A Definitions

Draft Date: 20 September 2001

Security Working Group Approval Date:

CCB Approval Date:

IT Modal Managers Approval Date:

IT Team Approval Date:

Revision Date:

Revision Number: 0

ACCESS The ability to interact with a process, network, or computing resource which permits the disclosure, use or manipulation of either the data processed by the resource, or the resource itself.

DATA OWNERSHIP Those individuals or organizations that originate, maintain, or have primary responsibility for information, and who have sole authority to authorize access to that data.

INFORMATION SECURITY PROGRAM The combination of the policies contained in this document, the documented procedures/practices to implement those policies, a security awareness program to educate all parties (owners and users) of their roles and responsibilities, and a security violation/investigation/reporting/resolution program.

LEAST PRIVILEGE The security concept that only the minimum level of access required to perform an authorized and legitimate job function shall be granted to a user, to be assigned to an individual while holding that job and to be revoked when the function is no longer performed by that individual.

Payment Card Industry (PCI) Compliancy that is adherence to a set of security standardsthat were developed to protect card information during and after a financial transaction.

Payment Card Industry Data Security Standards (PCI DSS) Proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.

Pen Test (Penetration Test) A tool for testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

PROCESS/RESOURCE OWNERSHIP Those individuals charged with maintaining a process, a network or a computing resource. Owners are responsible for the performance of the resource, which includes the implementation of security controls.

RISK The concept of evaluating the vulnerability of data, combined with the perceived threat to data, within the context of the value of the data, with the purpose of devising risk mitigation strategies.

SECURITY OF INFORMATION The person(s) responsible for establishing, enforcing, and administering security for a given computer resource.

SENSITIVITY OF INFORMATION The importance to the business, particularly with regard to potential harm resulting from inappropriate disclosure, corruption, or unavailability of the data. The sensitivity of data shall be determined by its Data Owner and communicated to all appropriate process/resource owners.

USERS Individuals with access to processes, networks or computing resources, as authorized by data owners and controlled by process/resource owners, for the purpose of using data contained within the system.

VULNERABILITY ASSESSMENT The systematic examination of a system/web server to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

Appendix B References

Annotated Code of Maryland, State Finance and Procurement Article, Sections 3-401 to 3-413 (Laws relating to information processing)

http://misc.state.md.us/cgi-win/web_statutes.exe

Annotated Code of Maryland, State government Article, Sections 10-611 through 10-701 (Laws relating to personal records, and records retention and disposal)

http://mlis.state.md.us/cgi-win/web_statutes.exe

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 7.0 World Wide Web (WWW)

http://csrc.nist.gov/isptg/html/ISPTG-7.html

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 8.0 Electronic Mail

http://csrc.nist.gov/isptg/html/ISPTG-8.html

Public Law 100-235, "Computer Security Act of 1987"

http://www.doc.gov/cio/oipr/csa-1987.html

Public Law 93-579, "The Privacy Act of 1974"

http://www.accessreports.com/statutes/PA.htm

Governor's Public Law 99-474, "Computer Fraud and Abuse Act of 1986"

http://www.panix.com/eck/computer-fraud-act.html

State of Maryland, Executive Order 01.01.194.18 "Privacy and State Data System Security"

http://www.usmh.usmd.edu/datasec/execord.html

United States Criminal Code 1030, "Fraud and Related Activity in Connection with Computers"

http://www.usdoj.gov/criminal/cybercrime/1030_new.html

Appendix C Forms and/or Disclaimers

1. MDOT Network Connection Terms and Conditions for Third Party Networks Disclaimer

Access between a third party network and the Maryland Department of Transportation (MDOT) network will be granted for lawful purposes only, limited to the scope of the service that is being provided to MDOT. Individuals from third party networks shall not transmit, retransmit, or store material or data that is the property of MDOT in violation of any federal or state laws.
Specifically prohibited acts by employees of third party networks include:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Unauthorized introduction of false information (public records).
6. Unauthorized disruption or interruption of the operation of a computer.
7. Unauthorized disruption of government operations or public services.
8. Unauthorized denial of services to authorized users.
9. Unauthorized taking or destroying data or software.
10. Unauthorized creating/altering a financial instrument or fund transfer.
11. Unauthorized misusing or disclosing passwords.
12. Unauthorized breaching a computer security system.
13. Unauthorized damaging, altering, taking or destroying computer equipment or supplies.
14. Unauthorized devising or executing a scheme to defraud.
15. Unauthorized obtaining or controlling money, property, or services by false pretenses.
16. Unauthorized disclosing of any info regarding the MDOT network such as IP addressing, design, etc.

Any hardware or software operated by a third party network that MDOT determines may cause hazard, interference, or service interruption to MDOT equipment, computers, or the MDOT network will be immediately disconnected by MDOT. Written notification can be provided after the equipment has been removed from the MDOT network explaining why this action was taken. This equipment will only be reconnected after corrective action is taken and MDOT has determined that the threat has been minimized or eliminated.

All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the MDOT Chief Information Officer, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, MDOT Office of Transportation Technology Services, designee or security officer.

I acknowledge that I have read, understand and agree to comply with the foregoing security advisory.

_____ _____
Name Printed or typed Signature

_____ _____
Name of Company Date

_____ _____
Printed typed Name of MDOT Project Manager Signature of MDOT Project Manager

Appendix D Incident Reporting

DBM Incident Report Form

Item	Guidelines
Incident Reference Numbers	Provide a unique incident number for each report. Reference any other applicable incident report numbers. (CERT)
Point of Contact Information	Provide as much POC information as possible; mailing address, e-mail address, telephone numbers (voice, pager, fax). (CERT, NIPC, FIWC)
Disclosure Information	Include a short disclosure or non-disclosure statement about what data should or should not be available to others. (CERT) Information may be shared with "The Public" or "InfraGard Members with Secure Access"? (NIPC)
Physical Location	Provide address for where the system is located. (NIPC, FIWC)
Mission/Mission Critical	What is the mission of the system involved? Is the system critical to the organization's mission? (NIPC, FIWC)
Operating System & Hardware	Provide operating system and hardware information. (NIPC, FIWC)
Security Measures	List what security measures are in place; firewall, IDS, auditing, encryption, etc. (NIPC, FIWC)
How Identified	How was the attack identified? (FIWC)
Hosts Involved	Include host names and IP addresses of sources and destinations involved. (CERT, NIPC, FIWC) Also, dumping data from whois and rwhois can provide additional information.
Description of Activity	Describe the activity. Were any vulnerabilities exploited, modifications made to the system, or software installed? (CERT) Was the attack a virus, denial of service, distributed denial of service, Trojan horse, trap door, or other? (NIPC) Actions attempted. (FIWC)
Evaluation of Attack Success	Did the attacker succeed in penetrating the system? Did damage result? (NIPC, FIWC)
Classification	List classification of system. Was any classified data compromised? (NIPC, FIWC)
Log Extracts	Include log entries that are related to the incident. Remove any unrelated entries to avoid confusion. If numerous log entries exist, include a sample of the entries and the total number of entries generated by the incident. Provide a description of the format may be helpful. (CERT)
Date/Time & Duration	Provide the date, time, and duration of the incident. (NIPC, FIWC)
Time Zone and Clock Accuracy	Provide the time in GMT offset to avoid international time zone confusion. State whether the times in the log are accurate or not. If not, state the difference. If the clock is synchronized with a time source,

	state so. (CERT)
Any Response Expected	State whether the report is for informational purposes only or if you are seeking assistance from an incident handler. (CERT)
Corrective Action	What actions have been taken to mitigate risk; disconnect, backup, checked binaries, etc.? (NIPC)

DoIT Guidance on Incident Reporting

Cybersecurity: Reportable Incidents – Additional Agency Guidance

Currently, DoIT security policy, in accordance with US-CERT and NIST guidelines, outlines specific incident reporting categories as delineated below.

Agency Incident Categories

Category	Type	Description
Category 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a state agency network, system, application, data, or other resource.
Category 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Category 3	Malicious Code	*Successful* installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
Category 4	Improper usage	A person violates acceptable computing use policies as defined in Section 11 of the DoIT Security Policy, v.3.1.

It is observed that several agencies are having some difficulty in defining incident *severity* and, therefore, do not have a consistent sense of when a security incident meets the threshold of a reportable event. To help agencies through this inexact science, we will again seek NIST guidance to align to a collection of impact and effort categories that will help to define when incidents should be reported to DoIT.

Consider the following tables:

Functional Impact Categories

Category	Definition	Reportable to DoIT
None	No effect to the organization's ability to provide all services to all users	N
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	N
Medium	Organization has lost the ability to provide a critical service to a subset of system users	Y

High	Organization is no longer able to provide some critical services to any users	Y

Information Impact Categories

Category	Definition	Reportable to DoIT
None	No information was exfiltrated, changed, deleted or otherwise compromised	N
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated	Y
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	Y
Integrity Loss	Sensitive or proprietary information was changed or deleted	Y

Recoverability Impact Categories

Category	Definition	Reportable to DoIT
Regular	Time to recovery is predictable with existing resources	N
Supplemented	Time to recovery is predictable with additional resources	Y
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	Y
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	Y

Effective immediately, please use this guidance for reporting security events to DoIT along with the catch-all condition of "anything beyond normal or out of the ordinary."

APPENDIX E: MDOT Breach Follow-up Policy

Purpose

The purpose of this policy is to define the steps that must be taken by the Maryland Department of Transportation's (MDOT) Transportation Business Units (TBUs) when a breach of an information system is confirmed. The TBUs will work closely with the InfoSec team and the MDOT Chief Information Officer (CIO) throughout this process.

An *incident* is defined as a security event that compromises the integrity, confidentiality, or availability of an information asset. When an incident results in the potential unauthorized disclosure of personal or confidential data, that is defined a *breach*. When a breach occurs resulting in release of data to an unauthorized party, this is defined as *data disclosure.*

The goal of this policy is to provide swift and thorough follow-up to any breached host and system, minimize any impact on any individuals whose information was disclosed, and to comply with both state and federal laws that address this policy. This action is taken in addition to the incident handling guidelines in Section 7 Security Incident Handling and Appendixes C.4 DBM Incident Report Form and C.5 DoIT Guide on Incident Handling.

Applicability

This policy applies to all MDOT TBU server administrators, TBU IT leads, and CIOs who are responsible for the administration and daily operations of a server or device that is breached. They will take responsibility to assure that the appropriate follow-up is taken with those impacted by the breach, and establish correspondence with any parties defined in this policy. Any alleged exposure or compromise of personally identifiable information (PII) or protected health information (PHI) will be investigated as a breach which is outlined in this policy.

PII is defined by NIST (NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information) as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity such as name, social security number, data and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information.

- Examples of PII include but are not limited to:
  Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristics), fingerprints, handwriting, or other biometric data.
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, educational information, financial information)

PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is outlined in the US Health Insurance Portability and Accountability Act (HIPAA).

Responsibilities

When a Security Incident occurs that is confirmed as a breach by the TBU CIO/IT Management that owns the impacted data, they will be responsible for taking follow-up action. The following steps must be taken:

1. Determine the cause of the breach. This is outlined in section 7.4 of the MDOT IT Security Plan, Security Incident Handling section. The cause of the breach, and the countermeasures implemented as corrective action must be documented.
2. Notify the MDOT CIO and MDOT IT Security Offices of the breach.
3. Notify the Office of the Attorney General at the ID Theft Hotline at 410-576-6491 or 410-576-6574 or via email to idtheft@oag.state.md.
4. Notify the Maryland Department of Information Technology. This is documented in Appendix C, item 4 – "MD DoIT Incident Response Form".
5. Identify and notify all impacted individuals of the breach. This can be done via written notice, telephone, or email. Records of this correspondence must be maintained.
6. Notification of the breach must be reported to a consumer reporting agency. Shown below are agencies that can be contacted:
7. Notify the banking institutions to ensure that their card brands are alerted of potential card brand incidents.

Consumer agencies to be notified in the event of a breach.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
http://www.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com
1-888-397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 98234
http://www.transunion.com
1-800-680-7289

Lifelock
60 East Rio Salado Parkway, suite 400
Tempe, AZ 85281
http://www.lifelock.com
1-800-607-7205

References for Card Brands Incident Reporting

VISA
http://usa.visa.com/merchants/protect-your-business/cisp/if-compromised.jsp

Mastercard
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

American Express
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=TH&tabbed=breach

Discover
http://www.discovernetwork.com/merchants/fraud-protection/

JCB
http://partner.jcbcard.com/security/jcbprogram/index.html

Appendix 5

MARYLAND DEPARTMENT OF TRANSPORTATION

INFORMATION SECURITY PLAN

Revision Date: 05/05/2017

Table of Contents

This document contains sensitive information; its contents are not to be shared without the written permission of the Maryland Department of Transportation Chief Information Officer.

1.1 Objective of Security Planning

The objective of system security planning is to improve protection of information technology (IT) resources. Maryland Department of Transportation (MDOT) systems have some level of sensitivity and require protection as part of good management practice. This document discusses the protection of MDOT information technology (IT) resources. The content provides security guidance in the form of subject matter security policies grouped together to form a basis for a security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

The purpose of this security plan is to provide an overview of the security requirements for the MDOT tangible and intangible assets. This document provides security guidance for security controls that are in place or are planned in order to strengthen the MDOT overall security posture. This system security plan also delineates responsibilities and expected behavior of all individuals who access MDOT IT resources. The intent of this security plan is to provide a living document that should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for use by all MDOT Agencies and departments and reflects input from various MDOT managers with responsibilities for various IT resources. Additional contributors include MDOT information owners, system administrators, system operators, end-users, and the Security Working Group for the MDOT. Updated information may be included in the basic plan and the structure and format will continue to be organized according to MDOT agency requirements as defined by the MDOT Security Working Group (SWG) beginning in early 2000.

This security plan will protect MDOT IT resources, if all Transportation Business Units (TBUs) of the MDOT review and continue to contribute requirements to the Security Working Group where necessary changes are authorized. All security relevant enhancements must be documented and authorized by the MDOT Change Advisory Board (CAB)on a weekly basis. This risk management component of MDOT provides an important quality control by authorizing proposed change control and accepting all residual risks ensuring a balance among continuity of operations, costs, and viable security solutions.

> **The security-planning document is based on an assessment of management, operational and technical controls and the authorization of the CAB in response to recommendations from modal representatives and the Security Working Group. An annual review of the entire security plan must be done and documented and a periodic recurring review of the guidance provided within this security plan must be carried out in response to any significant change that impacts the three main security attributes, namely, confidentiality, integrity, and availability. This security plan better positions the MDOT in ongoing efforts to strengthen security posture, and meeting fiduciary responsibility of due care and due diligence. Thus, MDOT is**

taking a proactive approach to information assurance through layered security that calls upon talent, technology, and tools.

1.2 History of This Document

The Information Systems Security Plan document is the result of a collaborative effort between the MDOT modal representatives and the SWG and is based on the requirements of the MDOT TBUs as submitted to the SWG. Work continues in crafting content and enhancing structure and format that complements existing MDOT documentation. Adoption of this document is contingent upon acceptance by the MDOT Change Advisory Board.

1.3 Organization of This Document

Security Policy is the basis for much of the security guidance within an organization, therefore this document is organized in a linear format with the subject matter content reflecting various specific security policies contributed from MDOT representatives. The SWG considered the content and appropriateness before making further changes during review sessions held monthly and the policies will eventually be available on MDOT intranet web sites for easy access.

1.4 Seven Areas of Security Useful For Policy and Planning

1.4.1 Physical Security

Physical security measures focus on the physical protection of a system or facility and the controls in place, which restrict access to system resources through:

- Access control systems that range from simple key locks to cipher locks and sophisticated key/swipe card systems, and biometric fingerprint readers.
- Keys, combinations and keycards that require the same level of protection afforded the most sensitive information processed or handled within the facility.

1.4.2 Environmental Security

- Fire suppression systems (sprinklers, fire extinguishers).
- Heating and air conditioning systems.
- Emergency lighting and power distribution systems.
- Controlled environment (temperature, humidity, air filtration).
- Manual procedures and practices designed to protect delicate equipment from damage.
- Prohibition of eating and drinking around computer equipment.

- Prohibition of smoking around equipment to eliminate a common source of damage to hard drives and potential for fires.

- Institution of good housekeeping practices to control dust and dirt around computer equipment.

1.4.3 Personnel Security

Personnel security practices are those steps taken to:

- Ensure the integrity and reliability of prospective system users and all other persons with access to sensitive infrastructure and information.

- Ensure user awareness and understanding of their individual security responsibilities.

1.4.4 Hardware Security

- Ensure the protection of the hardware components of a system.

- Maintenance of accurate and up-to-date inventories of all equipment.

- Procedures (property passes) that ensure accountability for all equipment.

- Procedures for securing or logically disconnecting equipment when idle or unattended

1.4.5 Software And Data Security

Security practices in these two areas focus on the manual practices and procedures implemented to complement the automated security controls that:

- Protect operating system software, applications software and database files.

- Protect (configuration/change management) application and operating system software throughout the development and integration processes.

- Provide assurance of the integrity and accuracy of the software.

- Continue software and data security practices throughout the system life cycle.

- Address the effective implementation, integration and administration of the various security features contained in the operating system, application, and database software.

1.4.6 Security Administration

Security administration practices include those measures associated with the implementation and administration of the computer security program. These practices include:

- Develop and implement comprehensive and effective security plans.
- Develop and test contingency and disaster recovery plans.
- Document all aspects of the security program.
- Develop and provide security training to all employees at all levels.
- Maintain a high level of user security awareness.

1.4.7 Procedural Security

Procedural security measures include manual controls implemented to supplement automated protection provided by infrastructure components by:

- Documentation of those measures and controls as a foundation to support secure system operations.
- Creation of an enterprise level Security Policy document that is based on a security risk assessment baseline that provides guidance for the creation of subsequent security documentation and supporting procedures.
- Includes the definitions, roles and responsibilities of all system users.
- Specifies the system security architecture and implementation.
- Specifies types of user activities.
- Describes other sets of manual procedures designed to ensure the safe and secure operation of networks and mainframe systems.

Section 2: Introduction

2.1 Critical Business Function

Information and information systems are necessary for the performance of just about every essential activity. Serious security problems with this information or these information systems could result in lost customers, reduced revenues, identity theft, compromise of data, and/or degraded reputation. As a result, information security must be a critical part of an MDOT's business environment.

2.2 Information Security Policies

An Information Security Policy is an imperative element of a complete information security plan that touches every part of MDOT where data is created, modified, stored or processed. Internet security demands the presence of policies that dictate how security products and devices are used to protect MDOT assets. Information Security is not about tools, but about risk assessment, management, and everyone exercising best practices. Therefore, sound security policies and practices help shore up defenses and thwart inadvertent or hostile attacks on the MDOT network. Adequate Information Security Policies that secure MDOT services creates trustworthiness that customers both demand and deserve.

Section 3: Remote Data Access Policy

3.1 Purpose

The purpose of this policy is to support the appropriate strategies for, and acceptable use of, remote access to Maryland Department of Transportation (MDOT) networks and network services and MDOT data. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT Chief Information Officer (CIO).

3.2 Scope

This policy applies to an individual, group of individuals, organizations, or companies who have been given authorization to access the Maryland Department of Transportation (MDOT) enterprise network/data remotely. This policy applies to all Transportation Business Units (TBUs), Agencies and/or Departments operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy follow a structured review and approval process.

For the purpose of this policy, Remote Access is defined as accessing non-public MDOT or TBU networks, computers, or computer services and applications (such as Web sites and Web-based applications and corporate data from a location that does not provide a direct connection (wired or wireless) to the MDOT/TBU Enterprise (internal) network/data. If at any time the connection must go through a network not provided by MDOT, the connection is considered remote access.

Public access to services, data, and applications made available on the Internet is not within the scope of this policy.

3.3 Policy Statement

Remote access is made available for administrative, management, enforcement, procurement, support, and maintenance functions. MDOT computers and networks provide access to numerous computing resources, many of which contain confidential data or contain devices that support public safety. Remote access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations. Users must also ensure the appropriate confidentiality of information retrieved and stored on remote devices.

.

3.4 Responsibilities

Each TBU is responsible for observing this policy or developing policy that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "Criminal Justice Information System (CJIS) Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

Remote Data Access Policy is developed by the MDOT sanctioned Security Working Group and submitted to Configuration Control Change Advisory Board (CAB) for interim approval. The MDOT CIO will present the proposed policy to the Information Technology Governance Board (ITGB) for review. The MDOT CIO will have final approval of the policy.

Approved Remote Data Access Policy is implemented under the direction of the MDOT Network Project Manager and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

The following sections define remote access responsibilities based on the role of the individual:

3.4.1 MDOT

MDOT will provide and centrally manage a Mobile Device Management Suite (MDM)[1]. This suite will enable technical controls to be managed on remote devices by MDOT. The MDM suite will force specific security functionality on remote devices such as password locks/timeouts, etc… At any time MDOT may find it necessary for security reasons to deregister a remote device, thereby cutting off access to the MDOT network. The above described functionality covers both personally owned and state owned equipment.

3.4.2 Remote Access User

Remote Access Users are defined as individual employees, contractors, or federal/state/local government employees who require remote access to MDOT networks and network services and corporate data. Remote Access Users are responsible for obtaining, completing, submitting, and observing requirements of the Remote Access Request Form.

[1] As of this update 01/09/14 An MDM suite has been purchased. TBU administrators have been trained and will be able to establish their policies for applications that would be available from mobile devices.

All Internet Remote Access Users are responsible for procuring, configuring, and installing a personal firewall, anti-virus protection software, and encryption software (as appropriate for sensitive data) on the device used to remotely connect to MDOT, if available. Remote Access Users are further responsible for keeping these protections up to date. Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities. Remote Users accept that their personally owned or MDOT provided mobile device will be managed via the MDM system. MDOT will load MDM software which allows MDOT the ability to remote disconnect and even wipe the device of MDOT info that is segmented out separately from their own information if it is a personal device.

The Remote Access User is responsible for installing, configuring, and maintaining any additional software required for establishing remote access communications, such as Virtual Private Network (VPN) clients or Secure Socket Layer (SSL) clients. Remote Access Users are also responsible for any additional software required to access network services, such as Citrix or other required software on their personal device.

The Remote Access User is responsible for the safekeeping of any devices assigned to the user for two-factor authentication, (such as hardware tokens mini-token, smart cards, etc.) and must report lost or stolen devices immediately to their Remote Access Administrator or TBU Service Desk. The Remote Access User may incur the cost of replacement devices.

The Remote Access User is responsible for reporting Remote Access Client or Application Software problems to their TBU Service Desk. The Remote Access User is also responsible for notifying the Remote Access Administrator that the connection either does or does not work upon completion of installation.

The Remote Access User is responsible for all system hardware and software maintenance to their remote device. MDOT and MDTA are not responsible for the condition of the remote Access User's personal remote device.

The Remote Access User's supervisor is responsible for notifying the Remote Access Administrator if and when the Remote Access User leaves state service, or is no longer working on behalf of an MDOT TBU in the case of a contractor.

3.4.3 TBU Supervisor

The TBU Supervisor is responsible for reviewing the Remote Access Request Form from the User and ensuring the user has correctly completed and signed the user portion of the form.

The TBU Supervisor authorizes the request by signing the Remote Access Request Form and specifying the types of access the User is granted. The TBU Supervisor then forwards the form to the TBU IT Office.

The TBU Supervisors will use MDOT approved technologies such as MDM, virtualization and remote control, to keep confidential data off mobile devices.

3.4.4 TBU Remote Access Administrator

The TBU Remote Access Administrator is responsible for coordinating activities associated with the Remote Access Request Form. He/she ensures the information on the form is correct and signed by the User, and the User's supervisor.

The TBU Remote Access Administrator is responsible for creating a remote access account for the user.

The TBU Remote Access Administrator is responsible for providing the User with all the passwords, configuration information, installation software and manuals required to access resources on the MDOT network remotely.

The TBU Remote Access Administrator is responsible for providing any required training to the Remote Access User on the use of applications required for Remote Access to the MDOT network

Each TBU Remote Access Administrator shall maintain a file, electronic or paper, containing the signed copies of the Remote Access Forms.

The Remote Access Administrator is responsible for notifying the user's supervisor when the account is setup.

The Remote Access Administrator is responsible for notifying the Remote Access User's Supervisor of violations of this and any acceptable use policy.

3.4.5 Remote Access Request Process

Figure 1 presents a diagram of the remote access request process.

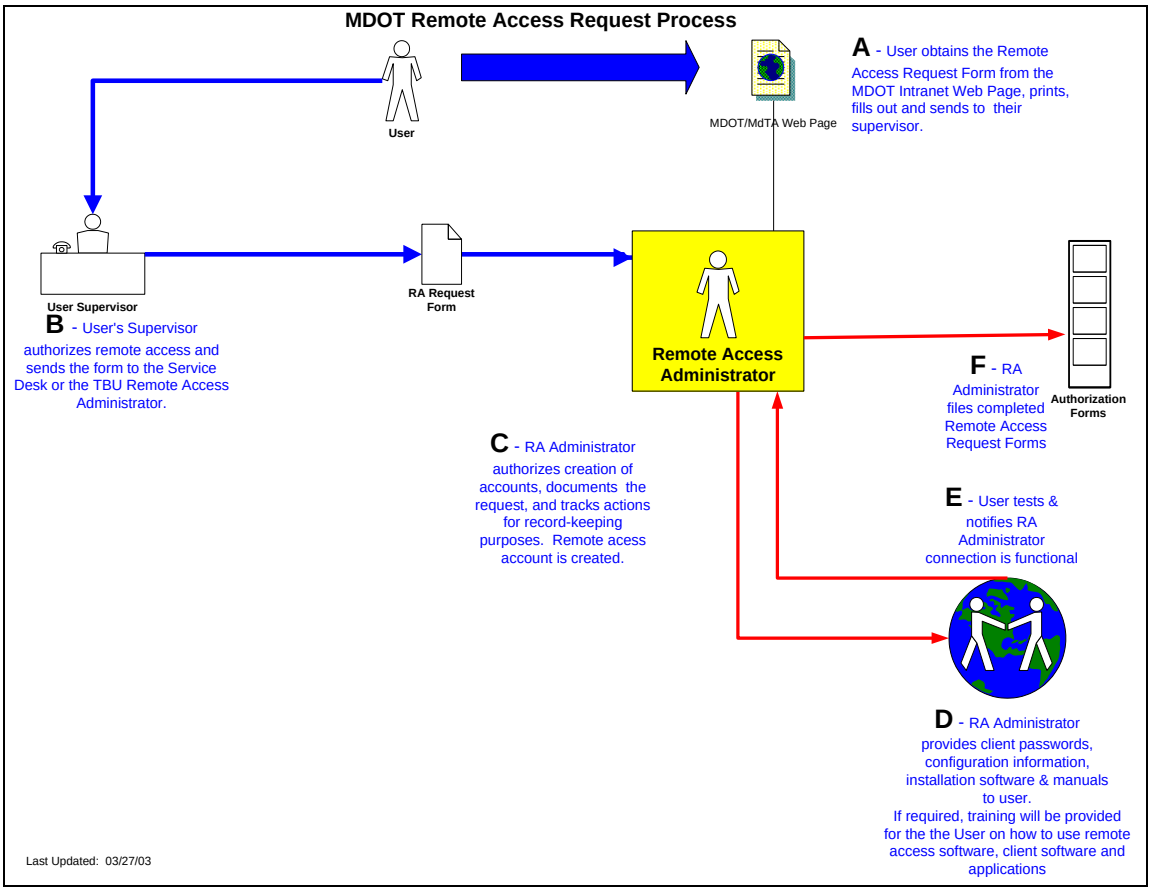

Figure 1 - Remote Access Request Process

3.5 Guidance

3.5.1 User or Individual Remote Access

An MDOT/TBU employee or individual contractor employee (User) requiring remote access to the MDOT/TBU network(s) and services initiates the Remote Access Request Process. The entity can obtain the Remote Access Request Form from the MDOT Intranet Web Page) or from the Remote Access Administrator. The User will print, complete and sign the User portion of the form and forward it to the User's Supervisor.

The User's Supervisor will review the User's request, authorize it and send the MDOT Remote Access Request Form to the TBU Service Desk or Remote Access Administrator.

The TBU Remote Access Administrator then reviews the request, ensures the Supervisor has correctly completed the Supervisor's section. The TBU Remote Access Administrator will ensure the request is documented and the actions are tracked in Maximo or another process for record-keeping purposes.

The TBU Remote Access Administrator then creates a remote access account for the user.

The TBU Remote Access Administrator maintains a file, electronic or paper, containing the completed MDOT Remote Access Request Form.

3.5.2 Third Party Remote Access

Request for remote access from organizations seeking a site-to-site connection over Internet-based Virtual Private Network (VPN) connections, or via direct telecommunication circuits will follow the guidance found in the "Third-party Access Policy".

3.5.3 Acceptable Use

Remote Access is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards activities;
- Communications for administrative purposes.
- Activities involved in the remote administration, support, or maintenance of MDOT/TBU network, computers, applications, and computing services
- Remote access to authorized systems and or data via the Internet

3.5.4 Remote Host Requirements for PCI Data Security Standards

In accordance with Payment Card Industry Data Security Standards (PCI DSS)[2], any MDOT employee or contractor remotely accessing a device that is in-scope with cardholder data must use a State-issued laptop with the following configuration in effect:

[2] PCI DSS Requirements and Security Assessment Procedures v3., 1.4, 1.4a, 1.4b (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf)

- Local firewall configured according to MDOT standards that cannot be changed by the laptop user.

- Local administrator account is not known or accessible by the laptop user.

- Local user account is for use by the laptop user and does not have access to change the firewall settings.

- Automatic updates setup for anti-virus, malware, and patches.

3.5.5 Restrictions

Remote Access may not be used for unlawful activities, commercial purposes not under the auspices of MDOT, personal financial gain, personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Remote Access:

- Private or personal, for profit activities (e.g., consulting for pay, sale of goods, charity fundraising);

- Solicitation of non-State business, or any use for personal gain or profit;

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

- At no time should any MDOT employee, contractor, or federal/state/local government employee provide their login or email password to anyone, not even family members.

- MDOT employees, contractors or federal/state/local government employee with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to the MDOT corporate network, is not connected to any other network at the same time

- Accessing or transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;

- Use for any purpose that is against State or Public policy or contrary to the State's best interest;

- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;

- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted

- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

- Misrepresenting in any manner, your identity, your account or a computing device in an Email or other electronic communication;

- Sending chain letters, advertisements, or solicitations of any type;

- Sending mass mailings to individuals who have not expressly agreed to be contacted in this manner;

- Knowingly sharing a personal account which includes use of a two-factor authentication device such as a token, grid card, soft token, etc.;

- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;

- Disclosing confidential or proprietary information.

- Use of any Dial-in desktop modems is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of remote control software is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of a network monitoring tool is prohibited unless specifically approved through the MDOT Change process-(CAB) Change Advisory Board

3.5.6 Representation

Remote Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

3.5.7 Interference

Remote Access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Remote Access systems. Such uses include, but are not limited to chain letters, "spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

3.5.8 No Expectation of Privacy

Privacy of Remote Access is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent, or received using the State's email system to authorized State supervisory personnel. The State affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations. The State shall make every reasonable effort to avoid viewing Union-related messages initiated by Union staff or bargaining unit members in accordance with Union agreements.

3.5.9 Security

The following specific guidance relating to Remote Access security is provided:

Strong Authentication

All users connecting from a remote host to the internal enterprise network must use two-factor authentication employing a method tested and approved by the Security Working Group.

VPN Encryption

All users connecting from a remote host to the internal enterprise network must use an encryption method that has been tested and approved by the Remote Access Group.

Virus Scan Software and Personal Firewalls

All users connecting from a remote host to the internal enterprise network must procure, install, and operate personal anti-virus and malware protection software. All users connecting from a remote host to the internal enterprise network via the Internet must procure, install and operate personal firewall software. Users should consult the INFOSEC group for guidance on acceptable approaches.

Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities.

All users connecting from a remote host to the internal enterprise network may be subject to a coordinated vulnerability assessment by MDOT or upon MDOT direction of their security contractor to test for proper security implementation at the remote host.

Authentication Token Policy

All users in possession of a security token are responsible for guarding and insuring the safekeeping of their token and must not share or redistribute tokens.

Users must report lost or stolen tokens to the remote access administrator or TBU Service Desk immediately. In the event a token is stolen, a police report must be filed for the missing article.

VPN Client Updates

VPN client updates are distributed to each TBU Remote Access Administrator and become the TBU Remote Access Administrator responsibility to distribute the update to their users.

Disclaimer

MDOT assumes no responsibility for any hardware, software, operating system problems, or the loss of any functionality or data to any personal user device used by any MDOT TBU Remote Access User.

3.5.10 Records Retention

State Records communicated using Remote Access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Remote Access system in accordance with each Department's standard practices.

Examples of Remote Access messages that typically are records include:

- Policies and directives,
- Correspondence or memoranda related to official business,

- Work schedules and assignments,
- Agendas and minutes of meetings,
- Drafts of documents that are circulated for comment or approval,
- Any document that initiates, authorizes, or completes a business transaction,
- Final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- Personal messages and announcements,
- Copies or extracts of documents distributed for convenience or reference,
- Phone message slips,
- Announcements of social events

Records communicated via Remote Access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

3.6 Definitions and Terminology

The following table defines the terms used to describe the various devices, entities or groups within this document.

The Network or Enterprise Network	MDOT and TBU network components.
Remote Access User	MDOT or TBU Employee/Contractor or Government Employee who has a job related/defined requirement to access the MDOT and TBU networks from a remote location.
Internet Users	Any remote access user connecting to the Enterprise network via an Internet Service Provider broadband connection from the Internet.
Transportation Business Units	The MDOT Transportation Business Units are defined as MDOT HQ (TSO), MAA, MDTA, MPA, MTA, MVA, SHA
MDOT	All TBUs (MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA) within the organizational structure of the MD Dept. of Transportation.
User's Supervisor	The User's Organizational Group Supervisor

IT COTR (Information Technology Contracting Officers' Technical Representative)	The IT COTR for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
Remote Access Administrator	The individual(s) designated as the Remote Access Administrator(s) for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
NOC	The MDOT Network Operations Center (NOC).
INFOSEC	The Information Security group within MDOT and its contractor

3.6.1 MDOT Remote Access Categories

Remote Access – Network Connection

This refers to remote access to the MDOT and TBU network that provides a direct connection to the network. This access requires two-factor authentication.

Remote Access – Service Access

This refers to remote access to the MDOT and TBU services and applications contained on the internal network. This access is offered through SSL connection via the MDOT Secure Portal (a form of secure reverse proxy)

Section 4: Password Policy

4.1 Purpose

The purpose of this policy is to insure when choosing a password, that it is extremely difficult for a potential intruder to make educated guesses about the selected password. This leaves the intruder no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a computer trying one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. In the event of a conflict between State, MDOT or TBU policy, the most stringent shall apply.

4.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, as well as any individual using MDOT resources. This policy applies to passwords required for all network and computer systems. Any device that requires an exception to this policy must be submitted and approved by the SWG.

4.3 Policy Statement

User accounts are provided for the purpose of conducting the business of this Agency and supporting the mission of each department. Computers and networks provide access to local and remote resources, as well as the ability to communicate with other users worldwide. Such open access is a privilege requiring individuals to act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

4.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement the policy. Each staff member with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

4.5 Guidance

The following are general password policies applicable for most systems and must be implemented if the system (operating system or software application) supports it:

Passwords and User IDs are unique to each authorized user.

Passwords for users-consist of a minimum of 8 alphanumeric characters (no common names or phrases). There shall be computer-controlled lists of prescribed password rules. Periodic testing to identify any password weaknesses (e.g., letter and number sequences, character repetition, initials, common words, and standard names) must be performed at least on a yearly basis where applicable.

The root or administrator account has a minimum password length of 11 characters.

Passwords are not the same as the User ID.

Passwords must not consist of all numbers, all special characters, or all alphabetic characters.

Users, Root and Administrators have at least one non-letter character in their password.

Passwords are changed every 45 days for users and every 30 days for system administrators. Most systems can enforce password change with an automatic expiration and prevent repeated or reused passwords.

Password history does not allow users to reuse any password in his/her last 10 attempts.

User accounts disabled after 4 consecutive failed login attempts.

Sessions suspended or locked by means such as a password-protected screensaver after 15 minutes of inactivity and require the password to be reentered to resume the session.

User accounts are disabled after 60 days of inactivity and deleted after 90 days of inactivity unless exempted by the TBU COTR or a manager of the TBU COTR.

User accounts are removed or disabled within 72 hours after notice to the TBU COTR that there has been termination of employment of the user.

Where applicable, successful logons should display the date and time of the last logon and logoff.

Users not allowed to use common passwords and passwords must not be based on personal information, i.e. username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.

Passwords are kept private i.e., not shared, coded into programs, or written down.

When an employee has a change in job duties and no longer needs access to a system, the account will be removed immediately.

4.5.1 Acceptable Use

Computers and networks are provided for the purpose of conducting the business of this Agency and to support the mission of each department. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with federal, state or local government personnel, vendors and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State association, government advisory or standard activities;
- Communications for administrative purposes
- Group or shared ids are prohibited unless they are documented as Steady State Accounts or Functional ID's. Steady State Accounts, Functional ID's are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., ACF2 id used to run production jobs). Passwords associated with functional ids are exempt from the password sharing and change requirements specified above

4.5.2 Restrictions

MDOT services may not be used for unlawful activities, commercial purposes not under the auspices of this Agency, personal financial gain, or personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines.

4.5.3 Representation

Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the MDOT or State

4.5.4 Interference

Services provided to MDOT shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or solicited interference with others' use of the systems provided

4.5.5 No Expectation of Privacy

Privacy of services such as email is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by MDOT. The State affords electronic mail privacy protections comparable to that which it traditionally afforded paper mail and telephone communications within the context of the State's legal and other obligations.

4.5.6 Security

Password security is the complete and sole responsibility of each individual. Users must take all reasonable precautions to prevent the use of the account by unauthorized individuals.

No user will be required to disclose his or her password.

Systems may be reviewed on a periodic basis to ensure the password policy compliance is being enforced.

4.5.7 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Section 5: External &Third-Party Networks Policy

5.1 Purpose

The purpose of this policy is to describe the "permitted uses", connection methods, and security controls for external (public) and remote, Third Party Networks connecting to the Maryland Department of Transportation (MDOT) network and devices.

The MDOT network allows access from the public to connect to their public servers that are located in the DMZ or service network. The DMZ (demilitarized zone) is a section of the network that resides between the public (untrusted) and the internal (trusted) network. Publicly accessible servers such as Web servers and FTP servers reside in the DMZ.

Third Party Networks are defined as networks that are not part of MDOT, or their network address space, requiring remote connectivity and access to devices within the MDOT Network. This policy also applies to Virtual Private Network (VPN) connections from MDOT to a Third-Party Network for accessing resources on their network. This policy requires that all Third Party Network connections will require the submission of a Remote Access Form as defined the in the guidance of Section 4, Remote Access Policy of the MDOT Security Plan. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

5.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, and to any individual using MDOT resources. This policy applies to all agencies and organizations connecting to the MDOT network.

5.3 Policy Statement

Network services are provided for the purpose of conducting the business of this Department and supporting the mission of each Transportation Business Unit (TBU). Computers and networks provide access to local and remote resources as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individuals act responsibly and observe all relevant laws, regulations and contractual obligations. All Third Party or External Networks are considered or assumed to be un-trusted and are subject to review and compliance with the requirements specified in this policy.

5.4 Responsibilities

Each TBU is responsible for developing policy that is entirely consistent with this MDOT policy, or adopting this policy as the TBU policy. The unique needs of each TBU's business

and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

5.5 Guidance

In strictly controlled situations, MDOT will allow Third Parties to access MDOT internal networks and computer systems. Both the owner of the MDOT information to which the Third Party will be granted access and the Third Party's Management Representative, must agree in writing, to such access before it is established. The Management Representative from the Third Party is also obligated to sign the MDOT Network Connection Terms and Conditions for Third Party Network Access" disclaimer (Appendix C). The decision-making process for granting such access includes consideration of the controls on the systems to be connected, the Third Party's security policies, and a network diagram of the relevant network segment(s) that will be connected to MDOT. The diagram, to be provided by the Third Party or developed internally must include the IP addresses, protocols, and equipment relevant to the connection.

MDOT will terminate the connection of Third Party network to the MDOT network at the conclusion or termination of a contract or project or at any such time that the connection is no longer required. With the approval of the Department CIO, MDOT reserves the right to terminate any connection in which a security breach is believed to be occurring or has occurred and corrective action has not been taken that meets the requirements of MDOT.

5.5.1 Acceptable Use

All network traffic passed from external networks must pass through an MDOT firewall. The following methods are accepted for permitting traffic from the public or Third-Party networks to MDOT's network:

Private leased line: A private leased line (e.g., frame relay, CCT1, TLS, etc.) can be connected from a Third-Party network to the MDOT vendor service network. The Third-Party network will be responsible for purchasing and providing the leased line service to include the circuit and associated hardware (routers, CSU/DSUs, cables, etc.) to establish the connection outside the MDOT network. Third Party responsibilities shall also include installation, maintenance, and problem solving of the network circuit and hardware. Network devices are preferred to be rack mountable. Device must be SNMPv2 manageable. Third Party is requested to provide MDOT, at a minimum, a read-only SNMPv2 Community String to permit device monitoring (CPU, memory, interfaces, etc.) by the MDOT Network Operation Center (NOC) network management tools. MDOT personnel are responsible for implementing the appropriate changes to the MDOT router(s) and MDOT firewall configuration to allow the traffic from the Third-

Party network to the entities within the MDOT network that is needed. Any data being passed through a private leased line that is deemed sensitive or critical must be encrypted. MDOT provides no security management of Third Parties connecting to this shared vendor service network. Vendors should provide their own security of that connection.

Internet from Third Party Networks: Any traffic being passed from the Third-Party network to MDOT using the Internet requires encryption. MDOT will require a Virtual Private Network (VPN) tunnel to be established from the Third-Party network to the MDOT enterprise firewall or to a VPN device/product used exclusively for that system approved by MDOT. The VPN must be established in one of the following methods: (a) firewall-to-firewall, (b) approved VPN client software to MDOT firewall, or (c) approved router to MDOT firewall. The VPN must employ IPSEC encapsulation; AES-256 encryption (Advanced Encryption Standard) and SHA5 hashing algorithm are required unless otherwise approved by the MDOT Security Working Group.

5.5.2 Internet from the public

All access from the general public to MDOT public servers must be terminated at the DMZ. The firewall must be configured to direct all traffic (including http/https) from the general public or from Third Party Networks only to the DMZ, creating a separation of the DMZ from the internal network. Any Web server in the DMZ that accepts or processes credit card payments are subject to PCI compliancy restrictions.

Network access granted by MDOT to the Third-Party network is restricted to only the hosts, protocols, and ports that are needed by the Third Party network in order to support their project or contract requirements. The Third-Party network is responsible for providing MDOT with this information in writing. All configuration changes made to MDOT network hardware or software are subject to review and approval of the MDOT Change Advisory Board (CAB). The MDOT CAB meets weekly to review and approve/disapprove network configuration updates.

Access granted from the public to servers in the MDOT DMZ are restricted to only the hosts and basic protocols that are required. All configuration changes needed for access from the public to the DMZ are subject to the review and approval for the MDOT CAB. Public servers in the DMZ are assigned a public IP address registered to MDOT which is translated to a private IP address assigned for the MDOT DMZ.

5.5.3 Acceptable and Prohibited Cryptographic Protocols and Cipher Suites

Cryptographic protocols are protocols that are designed to provide and assure secure communications offering privacy and encryption of data. The combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms that are used to negotiate the security settings for the cryptographic protocol is called a *cipher suite*. Over the course of time, protocols and cipher suites are

strengthened as hacking becomes sophisticated, thus older protocols are no longer recommended and supported. MDOT follows this paradigm to assure that a low risk factor exists in our network.

The following cryptographic protocols are not permitted in MDOT:

SSLv2, SSLv3, SSHv1

The TLSv1 cryptographic protocol is currently allowed but not preferred by MDOT. The following cryptographic protocols are permitted in MDOT:

TLS1.1, TLS1.2

The following weak cipher suites are not permitted in MDOT:

RC4, MD4, MD5, export-grade cipher suites

5.5.4 Representation

Third Parties shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT, TBU, or any unit of the State unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing MDOT or the State.

5.5.5 Interference

Services provided to MDOT and its TBUs shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive demand on any network resource or computing facilities, or unwarranted or unsolicited interference with others' use of the systems provided.

5.5.6 No Expectation of Privacy

Privacy of services and communications, such as email, is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by this Agency. The State does afford electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations.

5.5.7 Security

As a condition of access to MDOT's computer network, every Third-Party network must secure its own connected systems in a manner consistent with MDOT's requirements. MDOT reserves the right to immediately suspend network connections with Third Party systems not meeting such requirements or if security concerns arise, until those requirements are met.

All Third Party external network connections will be brought before the MDOT Security Working Group for review and approval. MDOT reserves the right to perform a network vulnerability assessment (scan) of any mission critical hosts on the Third-Party network after providing prior written notification of MDOT's intent to do so and specify a time range during which the scan will occur.

Routing of any private Internet Protocol addresses is prohibited. A private IP address is defined in RFC 1918, in which the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Public IP addresses are defined as those that have been legally registered through the InterNIC. MDOT will not route their registered IP addresses assigned to internal hosts over the Internet.

5.5.8 Records Retention

State Records must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Records communicated via Email are disposed of within the record keeping system in which they have been filed in accordance with [the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records.

Section 6: Kiosks Security Standards

The following standards should be followed whenever possible and if the facility can accommodate them.

6.1 Operating System Security

A. Password Protect the BIOS (8-character minimum, (larger when possible).

B. Operating System should the latest possible release of Windows whenever possible.

C. Operating System should auto-logon with a user account that has a password that adheres to the MDOT Security Policy for password complexity

D. The Administrator account should be renamed.

E. Block Internet access[3], assign a static IP address to Kiosk and remove DNS.

F. Create a Kiosk user profile and augment with policy editor.

1. Remove Run command from Start menu.
2. Remove folders from Settings on Start menu.
3. Remove Taskbar from Settings on Start menu.
4. Remove Find command from Start menu.
5. Hide drives on My Computer
6. Hide Network Neighborhood
7. Hide all items on Desktop
8. Disable Shutdown Command
9. Disable Registry Editing Tools

6.2 Physical Security

A. Configure switch port to only accept MAC address of Kiosk PC.

B. Bolt Kiosk in place.

C. Secure Kiosk access panels with commercial grade lock.

[3] When business reasons call for internet access, the MDOT Change Process will be followed to assure the necessary mitigation takes place.

D. Network cable should be placed in a conduit (ex. Greenfield) if the cable can't be run through the floor under the Kiosk.

E. Network cable should be permanently attached to the jack or encased in a strong locked cover if it is accessible.

F. Request the Kiosk to be placed in view of a security camera.

G. A physical site assessment must be performed by the MDOT Information Security team before the kiosk is approved for production and public accessibility. This must be noted in the Maximo Service Request. A letter stating the customer's knowledge of the visit and an attempt being made to challenge existing security procedures will be provided to the INFOSEC team doing the visit and signed by the customer.

Sample Customer Acknowledgement Letter.

October 09, 2013

To Whom It May Concern:

The MDOT (insert TBU name) has engaged personnel listed below to perform a vulnerability assessment and analysis beginning on MM/DD/YYYY and completing on MM/DD/YYYY. In the process of conducting this authorized exercise, the authorized personnel will ignore or challenge existing TBU and MDOT system security procedures as necessary to ensure that an effective assessment is performed. To verify the validity of this letter and authorized personnel, please check with the primary contact listed for the facility. If the primary contact cannot be located, please call [applicable client personnel and telephone number(s)] for verification.

This assessment is being performed at (list locations and/or list of network addresses)

AUTHORIZED PERSONNEL

NAME
NAME

LOCATION (S)	**PRIMARY CONTACT (S)**
As Applicable	As Applicable

Thank you for your cooperation.

Signature

Name of Client Authorized Manager

Title /Position
Telephone Number
Address

Section 7: Internet Web Hosting Policy

7.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to the Internet and provide public information access. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

7.2 Scope

This policy applies to all Internet Web server systems that are being built or in working condition regardless of whether they are hosted within MDOT or by a Third Party. Close attention should be made not only to the Web server itself, but also the security needs and requirements of the local network and other interconnected networks. In the case of collaborative efforts between MDOT and another governmental entity, MDOT management shall exercise due diligence to ensure that the intent of this policy is adhered to by the hosting party.

7.3 Policy Statement

There are many areas of Web servers to secure such as the underlying operating system, the Web server software, server scripts, and other associated components. All Agency Web servers that are accessible from the Internet must adhere to the following standards for operation and maintenance:

7.3.1 MDOT Hosting Policy:

1. Information placed on any Web site is subject to the same privacy restrictions as releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information.

2. A public Web server must not serve as a repository for confidential data, although it can act as a proxy for access to confidential data located on more secure hosts.

3. Users are forbidden to download, install or run Web server software without prior approval by the user's Agency authorized system administrator.

4. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

5. Web server software and the underlying operating system must employ all security patches and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

6. Place Web servers on subnets separate from internal networks.

7. Firewalls and routers must be in place and configured to restrict attacks from public and internal networks as well. Only traffic needed for browsing and business applications management is allowed through the firewall to access that server.

8. Since using a computer simultaneously as a public Web server and for other public Web services poses risks, a computer must be dedicated to the sole function as a Web Server. Specifically, business or personal files are vulnerable to a malicious Web user if access is gained to a directory on your computer.

9. Keep the computer free of any networked or shared drives to another system. Access to remote machines opens an avenue for a malicious user to breach security.

10. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users. Ensure MDOT password policy is followed.

11. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. A review of logs on a regular basis by authorized personnel to record and report anomalies to your organization's designated security point of contact is desirable.

12. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place.

13. An MDOT-approved Third Party will perform Web server security assessments bi-monthly unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes (not page content), etc. The Modal COTR and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

7.3.2 Third Party Hosting Policy:

MDOT hosting policies in sub-paragraphs 1, 2, 5, 7, 9, and 10 of paragraph 9.3.1 above also apply to Third Party Hosts. In addition, the following policies also apply:

1. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place. The Third-Party Host must be able to take off-line any portion of the Website that has been compromised.

2. The State will contract a Third Party to perform Web server security assessments after the initial assessment, at the discretion of MDOT, unless unforeseen events require immediate assessment. The Third-Party Host will provide written authorization for MDOT to perform these security assessments as part of the original contract. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal COTR, IT Manager and Third-Party Host will be informed before the assessment is done and receive a copy of the results.

3. Non-compliance with policy directives may result in revocation of the Web Hosting contract. Additionally, MDOT content will be removed from the server and MDOT will retain the rights to the domain name.

7.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

7.5 Guidance

This section establishes "high level" guidelines and standards supporting the agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

7.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

7.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 8: Intranet Web Hosting Policy

8.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to an Intranet. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of the Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

8.2 Scope

This policy applies to all Intranet Web server systems that are being built or in working condition regardless of whether they are hosted within the MDOT or by a Third Party. Close attention is required for the Web server as well as the security needs and requirements of the Intranet since they frequently house sensitive corporate information not intended to be viewed by anyone outside the Agency. Intranets clearly illustrate how challenges to security are not so much technical as they are procedural.

8.3 Policy Statement

There are many areas of Web servers to secure including the underlying operating system, the server software, server scripts, and other associated components. Noteworthy, Intranets require strict internal security policies and procedures to control access to sensitive corporate data from within. Even though Intranet Web servers are not accessible from the Internet, they remain susceptible to the same attacks including penetrations from the Internet via other systems on the "inside network", and also through Internet Web browsing from the server. All Agency Web servers must adhere to the following standards for operation and maintenance:

1. Information placed on any site is subject to the same privacy restrictions when releasing non-electronic information. Accordingly, before information is place on the Intranet, it must be reviewed and approved for release in the same manner as other official memos, reports or other official non-electronic information.

2. Users must not run Web server software without prior approval by a user's Agency-authorized System Administrator.

3. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

4. Server software and the underlying operating system must employ all security patches no later than one month of release and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

5. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users.

6. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. Additionally, authorized personnel must review logs regularly to record and report anomalies to your organization's designated Security Officer.

7. Procedures for Web Server users to report any dramatically unexpected changes on the site to system administrators or your organization's designated Security Officer must be in place.

8. A Third Party will perform Web server security assessments annually unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

8.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

8.5 Guidance

This section establishes "high level" guidelines and standards supporting the Agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

8.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

8.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed

and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 9: Wireless Communication Policy

9.1 Purpose

The purpose of this document is to define a policy for securing wireless connections within MDOT's network. Due to the inherently insecure nature of this technology, only secure wireless systems that meet the requirements in this policy are approved for connection to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

9.2 Scope

This policy applies to all MDOT employees, and staff subordinate to MDOT contracts. It is recommended that the "Policy Statement" be included in any contract award process. This policy covers all wireless networking devices (e.g., Wireless Access Points, bridges, computing devices, etc.) connected to any of MDOT's internal networks. Wireless devices and/or networks without any connectivity to MDOT's networks do not fall under the purview of this policy.

9.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. The security and integrity of this network must be upheld when utilizing wireless networking devices on the MDOT network.

In keeping with State of Maryland Department of Information Technology (DoIT) policy (Version 2.2) regarding Wireless (section 7.8), the following guidance will be observed:

- Establish a process for documenting all wireless access points
- Ensure proper security mechanisms are in place to prevent the theft, alteration. Or misuse of access points
- Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available
- Change default administrator credentials
- Change default SNMP strings if used, otherwise disable SNMP
- Change default SSID
- Deploy secure access point management protocols and disable telnet
- Strategically place and configure access points so that the SSID broadcast range does not exceed the physical perimeter of the building (unless the wireless solution is designed for providing outside connectivity).
- Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services

- Require wireless users to utilize encrypted data transmission if accessing internal LAN services

This MDOT/MDTA Wireless Communication Policy provides this additional guidance:

- No wireless access points shall be connected to the MDOT network without following the MDOT Change Management process.
- No end user device connected to the MDOT network (either wired or wireless) shall offer or allow connections to or from other networks
- No end user device will broadcast MDOT SSIDs or otherwise masquerade as a device providing connections to the MDOT network
- No MDOT wireless network management interfaces shall be accessible from the wireless network
- Wireless networks providing access to internal MDOT resources require WPA2 (Wi-Fi Protected Access - Enterprise) with two factor authentication.
- Wireless networks providing guest access to the Internet shall implement WEP (Wired Equivalent Privacy) at a minimum.
- Guest wireless network accounts will be unique and will be configured to expire passwords after eight hours. Exceptions to this policy must follow the MDOT Change Management process. For example, a one-week training class requiring guest wireless access may require an exception to the policy.

9.4 Responsibilities

Each Agency is responsible for developing procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

9.5 Guidance

All wireless networking devices providing a wired connection to the MDOT network must have approval from the Security Working Group and be submitted for review via the Change Management process prior to being connected to the MDOT network. Due to the highly evolving nature of this technology, an MDOT Wireless Standards document (see Appendix D) will be kept on an on-going basis that contains current MDOT implementations of these technologies, known issues, and recommendations.

Wireless devices found to be non-compliant with this or other appropriate policies (ie. Remote Access Policy, Email and Internet Use Policy) will have their connection terminated **immediately**.

Section 10: Secure FTP Policy

10.1 Purpose

The purpose of this policy is to support the appropriate use of secure and non-secure FTP access privileges for both MDOT and external users. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT/MDTA without the expressed written permission of the MDOT CIO.

10.2 Scope

This policy applies to an individual, government agency, or business-trading partner who has been given authorization to access the Maryland Department of Transportation (MDOT) Secure FTP Server from a remote site. This policy applies to all MDOT/MDTA Modal Agencies operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy will follow a structured review and approval process.

10.3 Terminology

The following table defines terms used to describe various devices, entities and groups within this document:

The Network or Enterprise Network	The combined MDOT Network and associated MDTA Network components.
Secure FTP Server	Private transfer file transfer system offering enterprise grade security.
MDOT	Maryland Department of Transportation
MDTA	Maryland Transportation Authority
NOC	Maryland Department of Transportation Headquarters
CCB	Configuration Control Board
CIO	Chief Information Officer
CCR	Configuration Change Request
DPPA	Driver's Privacy Protection Act
FTP	File Transfer Protocol

RDA	Records Disposition Authorization
SARA	State Archives and Records Administration

10.4 Policy Statement

Secure FTP access is made available for users and entities that are responsible for policy review, approval, implementation, enforcement, as well as equipment procurement and maintenance. Computers and networks provide access to remote resources, as well as the ability to communicate with other users worldwide. Open access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations.

MDOT HQ and the Configuration Advisory Board (CAB) are responsible for approving; implementing and enforcing the MDOT/MDTA Secure FTP Access Policy. The request is submitted to the Security Working Group for discussion and review. If agreed upon, the request is presented to the CAB. When accepted by the CAB, the request is presented to the IT Modal managers and, upon approval, is incorporated into this policy.

Secure FTP Access Policy is developed by the MDOT HQ sanctioned Security Working Group and submitted to MDOT CIO and the corresponding CCB for interim approval. The MDOT CIO will present the proposed policy to the IT Modal Managers/IT Teams for final review and approval.

Approved Secure FTP access Policy is implemented under the direction of the MDOT HQ and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

10.5 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The following sections define the Secure FTP Access responsibilities of the individuals listed below:

- Secure FTP access User
- System Administrator
- Secure FTP Access Administrator
- NOC Help Desk

10.5.1 Secure FTP Access User

Secure FTP Access Users are defined as business trading partners who require secure FTP access to the MDOT/MDTA Secure FTP Server.

If required, the Secure FTP user is responsible for obtaining the Request Form from the prospective MDOT/MDTA Modal Agency, completing and signing the first section of the Secure FTP access Request Form, and forwarding it to the Agency's Project Coordinator. Modal Agencies may assign this responsibility to their Project Coordinators.

The Secure FTP Access User is responsible for reporting Secure FTP access Client or Application Software problems to the appropriate Help Desk.

The Secure FTP access User is responsible for all system hardware and software maintenance to their personal computer. MDOT and MDTA are not responsible for the condition of the secure FTP access User's personal computer.

10.5.2 System Administrator

The Agency's System Administrator is responsible for reviewing the Secure FTP Access Request Form to ensure that the user has completed and signed the portion of the form designated for the user.

The System Administrator authorizes the request by signing the FTP Access Request Form and specifying the types of access the User will be granted. The Secure FTP Access Administrator who updates access controls processes the form.

10.5.3 Secure FTP Access Administrator

The Secure FTP Access Administrator is responsible for the following:

- Coordinating activities associated with the Secure FTP access Request Form. He/she ensures the information on the form is correct and signed by both the user and the Agency's System Administrator.
- Providing the NOC Help Desk with the information required in creating Secure FTP access directories. In this case, the Secure FTP Access Administrator faxes a copy of the Secure FTP access Request Form to the NOC Help Desk.
- Providing the User with passwords, configuration information, installation software, and manuals, required to access the Secure FTP Server remotely.
- Providing training to the Agency's Project Coordinator on the use of applications required for Secure FTP access, if required.
- Maintaining a file containing the signed copies of the Secure FTP Access Forms.
- Notifying the Agencies Project Coordinator when the account is setup.

10.6 NOC Help Desk

The NOC will provide priority level "Critical" support for Secure FTP Server specific problems as contractually agreed to with MDOT.

10.7 Guidance

A User wanting to access the MDOT Secure FTP Server must obtain authorization from the prospective MDOT Modal Agency. The User can obtain the Secure FTP Access Request Process from the Agencies FTP Access Administrator.

The Secure FTP client should complete, sign and return the following documents, if required by the Modal FTP Administrator:

- The Agency's FTP Driver's Privacy Protection Act (DPPA) compliance contract, which outlines the Users responsibilities under the Federal DPPA.
- Third Party External Communications Network Security Policy and MDOT Network Connection Terms and conditions for Third Party networks.
- The Agency's FTP Access Request Form.

Upon receipt and approval of the signed Secure FTP Documents, each Modal will transmit in a responsible and secure process, the Account User ID and password to either internal or external Users depending upon the location of the User. After the User signs on and modifies the default password, he/she should perform a verification test. Directions will be provided on whom to contact for lockouts of User ID and passwords if applicable.

10.8 Acceptable Use

Access to Secure FTP is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards;
- Communications for administrative purposes.

10.9 Restrictions

Secure FTP access may not be used for unlawful activities, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Secure FTP access:

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

- Transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;

- Use for any purpose that is against State or Public policy or contrary to the State's best interest;

- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;

- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

- Misrepresenting in any manner, your identity, your account or a computer in electronic communication;

- Knowingly sharing a personal account;

- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;

- Unauthorized Disclosure of confidential or proprietary information.

10.10 Representation

Secure FTP Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

10.11 Interference

Secure FTP access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Secure FTP access systems. Such uses include, but are not limited to chain letters, "Spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

10.12 No Expectation of Privacy

Privacy of Secure FTP Access is not guaranteed. Authorized State Employees may access and disclose the contents of all messages created, sent or received using the MDOT/MDTA Secure MDOT/MDTA Secure FTP Server.

10.13 Security

The following specific guidance relating to Secure FTP access security is provided:

- **Encryption**

All external users connecting to the Secure FTP server will use a minimum of 128-bit encryption. The server will only allow connections with 128-bit encryption or better if originating from an external network.

- **Disclaimer**

Modal Secure FTP Access Users are defined as Government Agencies or Businesses who require secure FTP access to the MDOT Server. Access to the MDOT Secure FTP server is considered a privilege.

MDOT assumes no responsibility for any hardware, operating system, or software application problems encountered by any MDOT Modal Secure FTP Access User when installing/using the designated security applications to connect to the MDOT Secure FTP Server.

10.14 Records Retention

Files transferred using Secure FTP access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Files

needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Secure FTP access system in accordance with each Department's standard practices.

Records transferred via Secure FTP access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

10.15 Secure FTP Access Administrators

Each Modal /Agency will assign their own Secure FTP Access Administrator.

Section 11: Vulnerability Assessment Scan Policy

11. 1 Vulnerability Assessment Scanning

11.1.1 Responsibilities

The Office of Transportation Technology Services (OTTS) IT Security office or the network managed services (NMS) contractor will perform server vulnerability assessment (VA) scans on a regular basis (scheduled or on request) unless unforeseen events require immediate assessment. Also, security assessments scans must be initiated after major application configuration changes. The Transportation Business Unit (TBU) Contracting Officers' Technical Representative (COTR) and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

11.1.2 Types of Scans

A *vulnerability assessment scan* is defined as a systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

A *discovery scan* runs on MDOT's subnets detecting all IP based hosts. Ports are scanned and services associated with those ports are enumerated. No vulnerabilities are determined during these scans.

A special Web server scan is run for Web servers that are located on the DMZ or internal MDOT network. This scan will crawl or spider each Web page, following all the links, perform code analysis, and perform vulnerability detection.

11.2 Frequency of VA scans

11.2.1 Pre-Production On Demand VA Scans

All new servers that are being placed in a production environment must pass a vulnerability assessment (VA) scan. The initial VA scans are performed by the server administrator/TBU management after the operating system is installed and ready for the test and development environment. This will give them the opportunity to remediate any vulnerabilities that are reported before submitting the request for the final scan to the OTTS IT Security or NMS contractor for the final scan. The final scan is performed by OTTS IT Security or NMS contractor personnel after the server is configured and the developer installs the application code onto the server, readying it for the production environment.

Additionally, assessments must be performed after major configuration changes deemed appropriate during the Security Review of the Change Request approval process.

11.2.2 Ongoing/Monthly Scheduled Scans

Vulnerability assessment scans of each TBU are run monthly. This consists of scanning all TBU resources including servers and workstations. During the scan, ports are scanned and services are enumerated. Based on the operating system, the assessment may require to login into the system or application, which requires credentials that are provided by the server administrator to be in place for the scan. All of the data gathered is processed through a very extensive matrix to determine vulnerabilities with remediation recommendations.

Discovery scans are also run ongoing throughout the network.

11.3 Criteria

The OTTS Office of IT Security or NMS contractor will determine based on the results of the scan whether the server passes or requires remediation. A risk score is provided in the report. Judgment is made on the severity of the vulnerability and the risk that it poses to the integrity of the MDOT network (likelihood of attack or exploitation).

The server administrator is expected to mitigate any of the vulnerabilities those are deemed to pose a high risk to the MDOT network. After remediation, another scan will be run to determine if the risk still exist. In cases where the server administrator/TBU management cannot remediate the vulnerability but requires placement of the server in the network, they must accept the risk and initiate a Safeguard Implementation Plan (SIP, Section 16) with the OTTS Office of IT Security.

11.4 Scans from Third Party Vendors

Any Web server that process or stores credit card data for online electronic transactions are subject to a scan to meet Payment Card Industry Data Security Standards (PCI DSS) requirements. The PCI scan must be performed by an external (Third-Party) Approved Scanning Vendor (APS). The TBU IT leads must arrange these scans with the OTTS Office of IT Security or NMS contractor, and make sure that the scheduled task is on the NOC calendar. A Service Request/Change Request must be opened if the scan requires temporary firewall changes to allow the scan to take place.

Any server(s) for which a TBU's business system or application is resident on that is hosted by a Third Party outside of the MDOT network must have a VA scan run quarterly by the Third-Party vendor. The vendor is responsible for providing the scan report to the TBU COTR and the OTTS Office of IT Security. The vendor is responsible for remediating any high or critical risk vulnerability under the direction of the OTTS Office of IT Security.

11.5 Communication of New Vulnerabilities

As new vulnerabilities are discovered or announced, the MDOT NMS InfoSec contractor or OTTS Security Team shall inform each COTR via email with a description of the vulnerability,

it's risk to the MDOT environment and where possible and practical, a means to mitigate or protect the TBU from the risk that the vulnerability presents. Sources of such vulnerability information include but are not limited to:

MS-ISAC

US-CERT

Vendor sites such as Cisco, Adobe, etc.

SANS Institute

Section 12: Computer and Network Equipment Disposal Policy

12.1 Purpose

The purpose of this policy is to describe the permitted disposal methods for devices that may contain data storage either on hard disk, removable media, or within memory. This includes, but is not limited to, computers, servers, routers, switches, copiers, printers, faxes, multipurpose devices, cameras, and other related equipment. Data left on hard drives, Random Access Memory (RAM), Flash Memory or Non-Volatile Memory can contain proprietary information or data that is sensitive to the security of the network and MDOT information. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

12.2 Scope

This policy applies to all MDOT and MDOT Transportation Business Units (TBUs) employees, and personnel subordinate to MDOT and TBU contracts. This applies to all network and stand-alone computer systems (desktops, workstations, laptops, and servers), routers, switches, hubs, concentrators, firewalls or other network related items. It also applies to systems not located within MDOT that are provided as a service to MDOT. Policy Statement

12.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. Proprietary and/or sensitive data may be permanently stored or cached on the hard drive, RAM, Flash Memory, or Non-Volatile Memory. Proper disposal of this data is required to protect the confidentiality of data and to ensure security of the network.

12.4 Responsibilities

Each Transportation Business Unit (TBU) is responsible for developing an expanded procedure that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT and State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

The MDOT CIO requires that each TBU send a report to the MDOT CIO Office that indicates specific information about equipment that has had to be "sanitized" prior to disposal. That information can be found on the MDOT NOC Portal under equipment sanitization reporting procedure.

12.5 Guidance

Once Computer and/or Network Equipment has been identified as "Excess for Disposal" the equipment will be advertised to all MDOT TBU for five (5) business days to determine if there is interest in acquiring the equipment. Any equipment that is to be reused by a TBU must have the hard drive wiped and reimaged. Any equipment not requested by a TBU will be disposed of as mandated in DGS' Inventory Standards & Support Services Division (ISSSD) Inventory Control Manual.

As stated in Section 6.4 of the Department of Information Technology's (DoIT's) Information **Security Policy Version 3.1; "**To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. The removed hard drives may either be sanitized with a disk wiping utility and re-used within an agency or must be physically destroyed such that they are permanently rendered functionally useless. Agency CIOs will be responsible for the hard drive removal, recycling, destruction and/or disposal process.

A request for waiver is to be submitted to DoIT's Enterprise Information Services for authorization of disposal of a device with a hard drive and/or electronic memory with justifying documentation to support that the media has been overwritten in accordance with U.S. Department of Defense media sanitization standards.

As stated in Section 6.5 of the Department of Information Technology's (DoIT) Information Security Policy version 3.1, "To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. Note: Disposal of electronic storage media should be in compliance with the agency's document retention policy and litigation hold procedures. Additionally, the procedures performed to sanitize electronic media should be documented and retained for audit verification purposes. This policy applies to all electronic storage media equipment that is owned or leased by the State (including, but not limited to: workstations, servers, laptops, cell phones and Multi-Function Printers/Copiers)."

Additional guidance will be provided using NIST Special Publication 800-88 Table A-1 Media Sanitization decision matrix.

Section 13: Network Access Policy

13.1 Purpose

The purpose of this policy is to describe the criteria a computer system must meet before being able to connect to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. Scope

This policy applies to anyone that needs to connect a microcomputer or server to the MDOT network including, but not limited to all MDOT employees, staff subordinate to MDOT contracts, and visitors. This applies to all computer systems (desktops, workstations, laptops, and servers) that need access to the MDOT network.

13.2 Policy Statement

Computers and networks provide access to MDOT and resources, as well as the ability to communicate with other users worldwide. All systems must be secure and up to MDOT standards before they will be allowed access to the network.

13.3 Responsibilities

Each Agency is responsible for developing policy and/or procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

13.4 Guidance

All computer systems must meet MDOT standards before access will be allowed on the MDOT network. MDOT has a policy of disabling unused network ports. The Modal Help Desk should be contacted to request access to the MDOT network and a Help Desk ticket will be created to ensure compliance with this policy. If currently disabled, the port will be activated within 24 hours of contacting the Help Desk. The following standards must be met before connection to the MDOT network is allowed.

- **Operating system patches up to date**

  Any microcomputer system and server must be up to date with the latest security patches for the operating system. The server administrator must apply all of the latest security patches and updates within a month after the updates are announced or immediately if the update is critical.

- **MDOT/MDTA has an account with administrative rights to the system**

Any microcomputer system and server that will be directly connected to the MDOT network longer than one day must have an MDOT account with administrative rights to the system accessible by the Modal technical staff. Any exceptions to this must be granted by the MDOT CIO in writing.

- **Antivirus Protection**

  Antivirus protection must be installed on the microcomputer system or server. The software must be configured to run at startup and stay memory-resident to check for viruses during normal activity. The software must also be up to date with the latest virus signatures.

If new and/or third-party systems (including laptops) need to be connected to the network in order to be patched, updated, or any other reason in order to meet MDOT standards, this activity can be performed by connecting to the secure build areas that are segregated from the MDOT network at the discretion of the Modal. It is the responsibility of the Third Party to update third-party systems.

Section 14: Safeguard Implementation Policy

14.1 Purpose

A. The State of Maryland Department of Transportation (MDOT) recognizes the need to mitigate and ultimately correct risks introduced to the MDOT Enterprise to the extent that it is plausible and possible.

B. MDOT further recognizes that it needs to be able to continue to serve its customers while mitigating or correcting a discovered risk to the enterprise unless the risk is so extreme that it requires immediate resolution to avoid potential loss or disclosure of critical IT Resources, Systems or Data.

C. MDOT requires Safeguard Implementation Plans to assist the organization in managing an identified risk in a controlled and structured manner. These plans contain information on risk details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to the identification of a specific risk(s) to the MDOT Enterprise.

14.2 Scope

A. This policy applies to the Maryland Department of Transportation (MDOT) organizations, their staff, and their contractors that manage and maintain computing devices and data communication devices that connect to the MDOT Enterprise Network.

14.3 Policy Statement

A. The Maryland Department of Transportation Office of Transportation Technology Services (OTTS) shall develop and maintain a Safeguard Implementation Plan (SIP) for any risk that is identified within the MDOT Enterprise[4].

B. The SIP will contain information pertinent to the nature and severity of the risk, a risk level rating, recommended controls, and selected controls for mitigating the risk. Additionally, a projected date for the implementation of each risk migration strategy will be stated and accepted by the parties responsible for the implementation of those strategies.

C. In the event that the risk is determined to be high and the required mitigating strategies cannot be implemented (not technically or financially feasible or cannot be implemented within a one-year period) the SIP documents will be accompanied by a "Management Risk Acceptance Memo" and signed by the Designated Approving Authority for the system in question, the Transportation Business Unit Chief Information Officer, and the MDOT Chief Information Officer.

[4] The Safeguard Implementation Plan shall use the NIST 800-30 Appendix C as a guide for gathering the required information.

D. The SIP and any associated Management Risk Acceptance Memos will be maintained and tracked by the MDOT Office of Transportation Technology Services (OTTS) Office of Data Security (OOS) to assure that the appropriate risk mitigation strategies are put in place in the time frames defined. The MDOT CIO and TBU CIO/Director of IT will be notified of any strategy that is in danger of not being completed or that may require an extension due to unforeseen circumstances.

14.4 Responsibilities

A. The Designated Approving Authority (DAA) is the application or system owner, responsible for assuring that vulnerabilities and associated risks are mitigated to the extent technically and financially feasible, within the milestones defined in the SIP. The DAA must also accept any remaining, or residual, risks associated with the application or system.

B. The Transportation Business Unit (TBU) Chief Information Officer, or his equivalent, shares the responsibilities of the Designated Approving Authority and accepts the risk on behalf of the TBU.

C. The MDOT Chief Information Officer, or his designee, is responsible for accepting risks for the MDOT Enterprise Network and for assuring that Safeguard Implementation Plans are adhered to.

D. The Office of Transportation Technology Services is responsible for coordinating and managing the risk and vulnerability assessment process as well as the creation, management, and monitoring of the SIP and associated documents including the "Authority to Operate" and the "Management Risk Acceptance Memo". This office is also responsible for maintaining this policy and any accompanying procedures.

14.5 Guidance

A. The Safeguard Implementation Plan seeks to follow the guidance provided in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-30 "Risk Management for Information Technology Systems".

14.6 Forms

A. Safeguard Implementation Plan

B. Vulnerability and Risk Assessment with Authority to Operate

C. Risk Acceptance Memo

Section 15: Cloud Computing Policy

15.1 Purpose

The National Institute of Standards and Technology (NIST) defines Cloud Computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.".

15.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) organizations and their staff, that wish to utilize Cloud base services. For the purposes of this policy it is relative to Software as a Service (SAAS), Hardware as a Service and Infrastructure as a service. The scope of this policy is only relevant to publicly available Cloud services, not any MDOT Corporate Cloud services that MDOT may or may not engage in.

15.3 Policy Statement

Cloud computing can offer benefits in the cost, performance, and delivery of information technology services and that the use of cloud computing services will grow significantly over time. This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of information technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Prior to procuring a cloud computing solution, the following issues must be considered in determining the appropriateness:

A. Relevant statutory and policy requirements for the system or data that is being considered, including privacy and personally identifiable information in the data. Resources, State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
B. Records management and retention requirements and the ability to comply under a cloud environment.
C. Procurement and financial implications - there is usually little upfront cost to these solutions but typically a monthly service fee associated with using the cloud solution. Consider the entire life-cycle costs.
D. Issue of interoperability with existing system(s).

15.4 Responsibilities

A. The Initiator of the request is responsible for submitting the Cloud Computing request form and assuring that all appropriate reviews and sign off's have occurred prior to submitting the Service Request. It should be noted that a cloud computing request form must be submitted for each new application or service being considered. Applications negotiated prior to the writing of the policy

B. The Designated IT Authority (DIA) is responsible for assuring that the data to be stored in a cloud based service has been properly classified using the MDOT Standard Data Classification template.

C The Designated Approving Authority (DAA) is responsible for providing the business justification and any cost information associated with using a Cloud based service to perform the business function. They are also the Agency Head or delegated authority for the business giving them the authority to approve the submission of the cloud computing request.

D. The request for using a Cloud based service will be submitted as a Normal Enterprise Change Request (CR) from the Service Request, which is reviewed by the MDOT NMS security, WAN, and systems sections and approved by the MDOT Change Manager. The Cloud Computing request form and the MDOT Standard Data Classification template is attached to the CR.

15.5 Guidance

The MDOT Cloud Computing policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing

Section 16: Mobile Device Access

16.1 Purpose

Mobile access to vital business applications and information empowers workers to be more productive, efficient, and flexible. This enables access to business systems and network resources from mobile devices such as smart phones and tablets. The access is controlled through a Mobile Device Management (MDM) tool to assure confidentiality, integrity, and availability.

16.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) Transportation Business Units (TBUs) and their staff that wish to utilize mobile devices to access the MDOT network. For the purposes of this policy it is relative to the centrally managed MDM suite in regard to granting access to employees and contractors. The mobile devices include smart phones and tablets that are both state-issued and personally owned (Bring Your Own Device or BYOD). Mobile devices that this policy applies to include iOS, Android, and Windows smartphones and tablets

16.3 Policy Statement

Mobile device access offer benefits by enabling MDOT employees and contractors to gain access to the network from their mobile devices, resulting in increased productivity and efficiency. There is also a risk that comes with this convenience, as the features that make smart devices beneficial to employees are also attractive to hackers, data thieves, malware distributors, and other criminals.

This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of Information Technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Mobile device access to the MDOT network is a privilege for authorized users. Users must sign the MDOT Mobile Device Management Acceptable Use Policy found in the appendix prior to being granted the access.

16.4 Guidance

The MDOT Mobile Device Management policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-124 - Guidelines on Managing the Security of Mobile Devices in the Enterprises.

16.5 Device Control

A mobile device serves many purposes, and can have personal and non-work related data stored within it. Also with the use of personally-owned devices (the BYOD concept), there is no assurance that the device is trustworthy. Organizations must assume that all mobile devices are un-trusted until proper measures to secure and monitor the device. The MDM is a technical solution that achieves degrees of trust in BYOD and State-issued devices. It also provides encryption of data in transit and on the device itself.

For personally-owned devices, all MDOT software and data will be maintained in a secure, isolated sandbox/secure container on the mobile device, separated from personal content on the device. This is known as *containerization.* A separate container for MDOT must be present on all mobile devices that are granted access to the MDOT network. This policy only applies to the MDOT container on the device set up by the MDM product, not to the entire device. (Note: for personally owned devices, some wireless carriers charge an extra fee if connecting to another network that passes through an MDM vendor).

For State-owned devices, containerization is not needed. These devices will be fully managed by the MDM and the TBU administrators.

16.6 Authentication Controls

All MDOT employees and contractors that are granted the privilege of using a mobile device to access the MDOT network are set up with a username and password through the MDM system. User accounts must not be shared with other individuals. The following password guidelines in accordance with MDOT and State DoIT are in place for authenticating to mobile devices:

1. New accounts must be set up with a pre-expiring password, forcing the user to create their own password.

2. Passwords must expire every 45 days.

3. The password length must be between 8 and 16 characters.

4. All passwords require an upper and lower-case letter, at least one number and at least one special character.

5. Any device that is idle for 15 minutes will be locked and require the password to be entered to unlock it.

6. User accounts will be disabled after 6 consecutive failed login attempts. Only the MDM administrators can unlock accounts.

16.7 Application Access

Mobile devices afford access to features that may be beneficial for work-related purposes. Some of these features include text messaging, a camera, GPS (Global Positioning System), and other apps. It is at the discretion of the TBU authorizer and MDM administrator to grant access to these features, which are maintained in the MDOT container of the device.

Access to the Internet (Web sites) will pass through the proxy server, enforcing the same controls in place for the employee/contractor working from a desktop. Mobile devices will have access to corporate email within the MDOT container of the device.

16.8 Compliancy Requirements

It is the responsibility of the mobile device user to maintain the most current version of software on their device. Users are responsible for assuring that the latest patches and versions on the device (state-owned or personal) must be present to assure the most sound security practices. This includes:

- The most current version of the MDM software.
- For smartphones, the device must have the most current IOS/Android software.
- Any applications present in the container.
- The MDM will automatically detect if a device has been jailbroken or rooted when logging onto the network. Any device that is detected as jailbroken or rooted will result in the container being erased. *Jailbreaking* is any third-party iPhone application which is installed and not approved by Apple. *Rooting* is unlocking the Android operating system so you can install unapproved (by Google) apps, update the OS, or replace the firmware.

16.9 Device Administration

All MDM administrators will be responsible for assigning the access needed for the users, creating the containers, providing any state-owned devices, and tracking usage. Any mobile device that is lost or stolen must be immediately reported by the user to their MDM administrator. Devices reported as lost or stolen must be wiped immediately.

Section 17: PCI Compliancy

17.1 Purpose

The purpose of this section is to identify all requirements that any TBU has which processes transactions involving credit and debit cards on their hosts in exchange for a service or product that they provide.

17.2 Scope

Any organization or merchant that accepts, transmits, or stores cardholder data (credit/debit cards) must be in compliance with Payment Card Industry Data Security Standards (PCI DSS). While the MDOT IT Security Plan addresses some of the policy subjects that are required for PCI DSS compliance, this section will provide the requirements that are specific for PCI DSS compliancy not addressed elsewhere in this plan.

17.3 Required Scans

Every quarter, any TBU that maintains an external-facing host or hosts that accepts, transmits, or stores cardholder data must undergo and pass a vulnerability scan from an external Approved Scanning Vendor (ASV). This involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network.

A scan must be conducted by an external scan (ASV or qualified personnel) after any significant change to Internet-facing hosts in the DMZ that store, process, or transmit cardholder data. According to PCI DSS requirement 11.2.3, "The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant"

On a quarterly basis, internal vulnerability assessment scans must be conducted on hosts that accepts, transmits, or stores cardholder data, or when a change is made to that host.

17.4 Penetration Tests

On an annual basis, a penetration test must be conducted by qualified personnel on any host that accepts, transmits, or stores cardholder data. Penetration tests must also be conducted after a significant change occurs on any host within scope of PCI (Cardholder Data Environment).

17.5 Wireless Guidelines

The wireless requirements for PCI DSS relate to whether or not the technology is part of the Cardholder Data Environment (CDE). The CDE is the computer environment where cardholder data is processed, transmitted, or stored and any networks or devices that are directly connected

to that environment. In accordance with PCI DSS Requirement 11.1 and 12.9, TBUs must check for and remove unauthorized wireless devices in the CDE on a regular basis, and maintain quarterly reports showing wireless scans of the network that may connect to the CDE which shows that rogue and unauthorized Wireless Access Points (WAPs) being eliminated, or have methodology in place that can detect authorized and unauthorized access points.

17.6 Network Security

In accordance with PCI DSS standard 1.1.6, firewall and/or router configuration for servers that accepts, transmits, or stores cardholder data must be restricted to the secure Internet Protocols of HTTPS (port 443), SSH (port 22) {note – check PCI DSS 3.1 regarding SSH}, or must be passed across a Virtual Private Network (VPN). Firewall and router configuration must be reviewed bi-annually to assure that the CDE is maintained up to standard.

17.7 Encryption

In accordance with PCI DSS standard 4.1, strong cryptography must be present to safeguard sensitive cardholder data over open, public networks. All hosts that accept, process, or store cardholder data must have an SSL certificate from a trusted Certificate Authority (CA) vendor. These hosts must have the Transport Layer Security (TLS) encryption protocol in place {note: review language with TLS}.

17.8 Access and Maintaining Cardholder Data

Access to any cardholder data must be restricted to only those individuals that require it for business purposes. If the Primary Account Number (PAN) is ever displayed, it must be *masked*, meaning that only up to the first six or the last four digits of the account number can be viewed. No individual will have access to data displaying the full PAN without written consent from the TBU's CIO. A designated manager or director from each TBU must maintain a list of individuals that have access to data with the full PAN, their role and business purpose for that access. This list must be reviewed quarterly to determine if any changes are needed.

In accordance with PCI DSS standard 3.4, any TBU that stores cardholder data must have a data retention and disposal policy in place established. Any credit or debit card numbers that are stored must be rendered unreadable if storage is required.

Appendix A Definitions

Draft Date: 20 September 2001

Security Working Group Approval Date:

CCB Approval Date:

IT Modal Managers Approval Date:

IT Team Approval Date:

Revision Date:

Revision Number: 0

ACCESS The ability to interact with a process, network, or computing resource which permits the disclosure, use or manipulation of either the data processed by the resource, or the resource itself.

DATA OWNERSHIP Those individuals or organizations that originate, maintain, or have primary responsibility for information, and who have sole authority to authorize access to that data.

INFORMATION SECURITY PROGRAM The combination of the policies contained in this document, the documented procedures/practices to implement those policies, a security awareness program to educate all parties (owners and users) of their roles and responsibilities, and a security violation/investigation/reporting/resolution program.

LEAST PRIVILEGE The security concept that only the minimum level of access required to perform an authorized and legitimate job function shall be granted to a user, to be assigned to an individual while holding that job and to be revoked when the function is no longer performed by that individual.

Payment Card Industry (PCI) Compliancy that is adherence to a set of security standardsthat were developed to protect card information during and after a financial transaction.

Payment Card Industry Data Security Standards (PCI DSS) Proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.

Pen Test (Penetration Test) A tool for testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

PROCESS/RESOURCE OWNERSHIP Those individuals charged with maintaining a process, a network or a computing resource. Owners are responsible for the performance of the resource, which includes the implementation of security controls.

RISK The concept of evaluating the vulnerability of data, combined with the perceived threat to data, within the context of the value of the data, with the purpose of devising risk mitigation strategies.

SECURITY OF INFORMATION The person(s) responsible for establishing, enforcing, and administering security for a given computer resource.

SENSITIVITY OF INFORMATION The importance to the business, particularly with regard to potential harm resulting from inappropriate disclosure, corruption, or unavailability of the data. The sensitivity of data shall be determined by its Data Owner and communicated to all appropriate process/resource owners.

USERS Individuals with access to processes, networks or computing resources, as authorized by data owners and controlled by process/resource owners, for the purpose of using data contained within the system.

VULNERABILITY ASSESSMENT The systematic examination of a system/web server to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

Appendix B References

Annotated Code of Maryland, State Finance and Procurement Article, Sections 3-401 to 3-413 (Laws relating to information processing)

http://misc.state.md.us/cgi-win/web_statutes.exe

Annotated Code of Maryland, State government Article, Sections 10-611 through 10-701 (Laws relating to personal records, and records retention and disposal)

http://mlis.state.md.us/cgi-win/web_statutes.exe

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 7.0 World Wide Web (WWW)

http://csrc.nist.gov/isptg/html/ISPTG-7.html

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 8.0 Electronic Mail

http://csrc.nist.gov/isptg/html/ISPTG-8.html

Public Law 100-235, "Computer Security Act of 1987"

http://www.doc.gov/cio/oipr/csa-1987.html

Public Law 93-579, "The Privacy Act of 1974"

http://www.accessreports.com/statutes/PA.htm

Governor's Public Law 99-474, "Computer Fraud and Abuse Act of 1986"

http://www.panix.com/eck/computer-fraud-act.html

State of Maryland, Executive Order 01.01.194.18 "Privacy and State Data System Security"

http://www.usmh.usmd.edu/datasec/execord.html

United States Criminal Code 1030, "Fraud and Related Activity in Connection with Computers"

http://www.usdoj.gov/criminal/cybercrime/1030_new.html

Appendix C Forms and/or Disclaimers

1. MDOT Network Connection Terms and Conditions for Third Party Networks Disclaimer

Access between a third party network and the Maryland Department of Transportation (MDOT) network will be granted for lawful purposes only, limited to the scope of the service that is being provided to MDOT. Individuals from third party networks shall not transmit, retransmit, or store material or data that is the property of MDOT in violation of any federal or state laws.
Specifically prohibited acts by employees of third party networks include:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Unauthorized introduction of false information (public records).
6. Unauthorized disruption or interruption of the operation of a computer.
7. Unauthorized disruption of government operations or public services.
8. Unauthorized denial of services to authorized users.
9. Unauthorized taking or destroying data or software.
10. Unauthorized creating/altering a financial instrument or fund transfer.
11. Unauthorized misusing or disclosing passwords.
12. Unauthorized breaching a computer security system.
13. Unauthorized damaging, altering, taking or destroying computer equipment or supplies.
14. Unauthorized devising or executing a scheme to defraud.
15. Unauthorized obtaining or controlling money, property, or services by false pretenses.
16. Unauthorized disclosing of any info regarding the MDOT network such as IP addressing, design, etc.

Any hardware or software operated by a third party network that MDOT determines may cause hazard, interference, or service interruption to MDOT equipment, computers, or the MDOT network will be immediately disconnected by MDOT. Written notification can be provided after the equipment has been removed from the MDOT network explaining why this action was taken. This equipment will only be reconnected after corrective action is taken and MDOT has determined that the threat has been minimized or eliminated.

All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the MDOT Chief Information Officer, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, MDOT Office of Transportation Technology Services, designee or security officer.

I acknowledge that I have read, understand and agree to comply with the foregoing security advisory.

_____ _____
Name Printed or typed Signature

_____ _____
Name of Company Date

_____ _____
Printed typed Name of MDOT Project Manager Signature of MDOT Project Manager

Appendix D Incident Reporting

DBM Incident Report Form

Item	Guidelines
Incident Reference Numbers	Provide a unique incident number for each report. Reference any other applicable incident report numbers. (CERT)
Point of Contact Information	Provide as much POC information as possible; mailing address, e-mail address, telephone numbers (voice, pager, fax). (CERT, NIPC, FIWC)
Disclosure Information	Include a short disclosure or non-disclosure statement about what data should or should not be available to others. (CERT) Information may be shared with "The Public" or "InfraGard Members with Secure Access"? (NIPC)
Physical Location	Provide address for where the system is located. (NIPC, FIWC)
Mission/Mission Critical	What is the mission of the system involved? Is the system critical to the organization's mission? (NIPC, FIWC)
Operating System & Hardware	Provide operating system and hardware information. (NIPC, FIWC)
Security Measures	List what security measures are in place; firewall, IDS, auditing, encryption, etc. (NIPC, FIWC)
How Identified	How was the attack identified? (FIWC)
Hosts Involved	Include host names and IP addresses of sources and destinations involved. (CERT, NIPC, FIWC) Also, dumping data from whois and rwhois can provide additional information.
Description of Activity	Describe the activity. Were any vulnerabilities exploited, modifications made to the system, or software installed? (CERT) Was the attack a virus, denial of service, distributed denial of service, Trojan horse, trap door, or other? (NIPC) Actions attempted. (FIWC)
Evaluation of Attack Success	Did the attacker succeed in penetrating the system? Did damage result? (NIPC, FIWC)
Classification	List classification of system. Was any classified data compromised? (NIPC, FIWC)
Log Extracts	Include log entries that are related to the incident. Remove any unrelated entries to avoid confusion. If numerous log entries exist, include a sample of the entries and the total number of entries generated by the incident. Provide a description of the format may be helpful. (CERT)
Date/Time & Duration	Provide the date, time, and duration of the incident. (NIPC, FIWC)
Time Zone and Clock Accuracy	Provide the time in GMT offset to avoid international time zone confusion. State whether the times in the log are accurate or not. If not, state the difference. If the clock is synchronized with a time source,

	state so. (CERT)
Any Response Expected	State whether the report is for informational purposes only or if you are seeking assistance from an incident handler. (CERT)
Corrective Action	What actions have been taken to mitigate risk; disconnect, backup, checked binaries, etc.? (NIPC)

DoIT Guidance on Incident Reporting

Cybersecurity: Reportable Incidents – Additional Agency Guidance

Currently, DoIT security policy, in accordance with US-CERT and NIST guidelines, outlines specific incident reporting categories as delineated below.

Agency Incident Categories

Category	Type	Description
Category 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a state agency network, system, application, data, or other resource.
Category 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Category 3	Malicious Code	*Successful* installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
Category 4	Improper usage	A person violates acceptable computing use policies as defined in Section 11 of the DoIT Security Policy, v.3.1.

It is observed that several agencies are having some difficulty in defining incident *severity* and, therefore, do not have a consistent sense of when a security incident meets the threshold of a reportable event. To help agencies through this inexact science, we will again seek NIST guidance to align to a collection of impact and effort categories that will help to define when incidents should be reported to DoIT.

Consider the following tables:

Functional Impact Categories

Category	Definition	Reportable to DoIT
None	No effect to the organization's ability to provide all services to all users	N
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	N
Medium	Organization has lost the ability to provide a critical service to a subset of system users	Y

High	Organization is no longer able to provide some critical services to any users	Y

Information Impact Categories

Category	Definition	Reportable to DoIT
None	No information was exfiltrated, changed, deleted or otherwise compromised	N
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated	Y
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	Y
Integrity Loss	Sensitive or proprietary information was changed or deleted	Y

Recoverability Impact Categories

Category	Definition	Reportable to DoIT
Regular	Time to recovery is predictable with existing resources	N
Supplemented	Time to recovery is predictable with additional resources	Y
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	Y
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	Y

Effective immediately, please use this guidance for reporting security events to DoIT along with the catch-all condition of "anything beyond normal or out of the ordinary."

APPENDIX E: MDOT Breach Follow-up Policy

Purpose

The purpose of this policy is to define the steps that must be taken by the Maryland Department of Transportation's (MDOT) Transportation Business Units (TBUs) when a breach of an information system is confirmed. The TBUs will work closely with the InfoSec team and the MDOT Chief Information Officer (CIO) throughout this process.

An *incident* is defined as a security event that compromises the integrity, confidentiality, or availability of an information asset. When an incident results in the potential unauthorized disclosure of personal or confidential data, that is defined a *breach*. When a breach occurs resulting in release of data to an unauthorized party, this is defined as *data disclosure.*

The goal of this policy is to provide swift and thorough follow-up to any breached host and system, minimize any impact on any individuals whose information was disclosed, and to comply with both state and federal laws that address this policy. This action is taken in addition to the incident handling guidelines in Section 7 Security Incident Handling and Appendixes C.4 DBM Incident Report Form and C.5 DoIT Guide on Incident Handling.

Applicability

This policy applies to all MDOT TBU server administrators, TBU IT leads, and CIOs who are responsible for the administration and daily operations of a server or device that is breached. They will take responsibility to assure that the appropriate follow-up is taken with those impacted by the breach, and establish correspondence with any parties defined in this policy. Any alleged exposure or compromise of personally identifiable information (PII) or protected health information (PHI) will be investigated as a breach which is outlined in this policy.

PII is defined by NIST (NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information) as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity such as name, social security number, data and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information.

- Examples of PII include but are not limited to:
  Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristics), fingerprints, handwriting, or other biometric data.
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, educational information, financial information)

PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is outlined in the US Health Insurance Portability and Accountability Act (HIPAA).

Responsibilities

When a Security Incident occurs that is confirmed as a breach by the TBU CIO/IT Management that owns the impacted data, they will be responsible for taking follow-up action. The following steps must be taken:

1. Determine the cause of the breach. This is outlined in section 7.4 of the MDOT IT Security Plan, Security Incident Handling section. The cause of the breach, and the countermeasures implemented as corrective action must be documented.
2. Notify the MDOT CIO and MDOT IT Security Offices of the breach.
3. Notify the Office of the Attorney General at the ID Theft Hotline at 410-576-6491 or 410-576-6574 or via email to idtheft@oag.state.md.
4. Notify the Maryland Department of Information Technology. This is documented in Appendix C, item 4 – "MD DoIT Incident Response Form".
5. Identify and notify all impacted individuals of the breach. This can be done via written notice, telephone, or email. Records of this correspondence must be maintained.
6. Notification of the breach must be reported to a consumer reporting agency. Shown below are agencies that can be contacted:
7. Notify the banking institutions to ensure that their card brands are alerted of potential card brand incidents.

Consumer agencies to be notified in the event of a breach.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
http://www.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com
1-888-397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 98234
http://www.transunion.com
1-800-680-7289

Lifelock
60 East Rio Salado Parkway, suite 400
Tempe, AZ 85281
http://www.lifelock.com
1-800-607-7205

References for Card Brands Incident Reporting

VISA
http://usa.visa.com/merchants/protect-your-business/cisp/if-compromised.jsp

Mastercard
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

American Express
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=TH&tabbed=breach

Discover
http://www.discovernetwork.com/merchants/fraud-protection/

JCB
http://partner.jcbcard.com/security/jcbprogram/index.html