TASK ORDER REQUEST FOR PROPOSALS (TORFP)
AGILE SCRUM TEAM RESOURCES
OTHS/MDTHK-18-009-S N00P8400064
AMENDMENT #5

SEPTEMBER 12, 2017

Prospective Offerors:

This amendment is being issued to amend certain information in the above named RFP. All information contained herein is binding on all Offerors who respond to this RFP. The changes are listed below. New language has been double underlined and marked in bold (i.e., **word**) and language that has been deleted has been marked with a strikethrough (i.e. word).

1. Revise Attachment 1 – Price sheet as follows:

   (TAB 2- Key Personnel Labor Rates) -The formula cell C11 has been revised from /~~3~~ to /**5**

2. Revise TABLE OF CONTENTS LIST OF ATTACHMENTS as follows: Add
   - **ATTACHMENT 14 – SAFEGUARDING INFORMATION FROM THE UNITED STATES INTERNAL REVENUE SERVICE**
   - **ATTACHMENT 15- ANNUAL INTERNAL REVENUE SERVICE EMPLOYEE AWARENESS**
   - **ATTACHMENT 15-1- UNAUTHORIZED DISCLOSURE OF INFORMATION**
   - **ATTACHMENT 15-2- CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION**
   - **ATTACHMENT 15-3- REPORTING IMPROPER INSPECTIONS OR DISCLOSURES**
   - **ATTACHMENT 16- BACKGROUND CHECK AFFIDAVIT**
   - **APPENDIX -4 MDTHINK PLATFORM**
   - **APPENDIX -5 MDTHINK INFRASTRUCTURE**

3. Revise LIST OF ATTACHMENTS Table as follows: Add

Attachment 14	**Safeguarding Information from the U.S. Internal Revenue Service**	**Submit with Work Order**
Attachment 15	**Annual Internal Revenue Service Employee Awareness**	**Submit with Work Order**
Attachment 15-1	**Unauthorized Disclosure of Information**	**Do Not Submit with Proposal or Work Order**
Attachment 15-2	**Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information**	**Do Not Submit with Proposal or Work Order**
Attachment 15-3	**Reporting Improper Inspections**	**Do Not Submit with Proposal or**

	or Disclosures	**Work Order**
Attachment 16	**Background Check Affidavit**	**Submit with Work Order Award**

4. Revise Section 1.11 TRAVEL REIMBURSEMENT as follows: Expenses for travel performed in completing tasks for this TORFP shall be **included as part of the fully loaded hourly labor rate for each labor category** ~~reimbursed~~ in accordance with ~~the CATS+ RFP~~ **ATTACHMENT 1- PRICE PROPOSAL Instructions**.

5. Revise Section 3.9 REQUIRED POLICIES, GUIDELINES AND METHODOLOGIES. Add the following section:

(G) DHS Security Policy: Below are the minimum requirements to obtain OTHS approval for devices to be *connected to* DHS systems. These requirements are the minimum as of May 4, 2017, but will change as federal requirements and security standards evolve. Vendors are required to ensure that their equipment meets minimum requirements as they evolve.

- **Windows 7 Professional 64-bit (or later) with all current security patches and ongoing monthly patches for operating systems and applications;**
- **Current antivirus solution that is maintained and patched daily;**
- **USB ports must be protected such that no non-FIPS compliant hardware level encryption devices that can store data can connect to the laptop, desktop or tablet;**
- **Office Productivity Suite: Microsoft Office 2007 Professional;**
- **Computers must automatically lock after periods of inactivity. The period of inactivity prior to locking will be no greater than 15 minutes for devices containing DHS data;**
- **Laptops must have Absolute Computrace or another endpoint security that can be used to track, freeze, and remotely wipe the device;**
- **Portable Media Devices, including laptops, must have FIPS 140-2 Compliant Hardware Level encryption; and**
- **All data must be wiped prior to separation from DHS.**

In addition, any breach of the DHS system or DHS data, including theft or loss of a portable device, must be reported to the OTHS Helpdesk within 1 hour of discovery of the theft/loss/breach. The OTHS Helpdesk can be reached at 410-767-7002.

OTHS reserves the right to audit these requirements at any time and/or deny connectivity to DHS systems.

6. Add Section **3.15 Security Clearance / Criminal Background Check**

3.15.1 The Contractor shall obtain from each prospective employee, a signed statement permitting a criminal background check.

3.15.2 The Contractor shall obtain a Criminal Justice Information System (CJIS) State and Federal criminal background check, which shall include at a minimum: fingerprinting, a check of local law enforcement records where the individual has lived, worked, or attended school within the last five (5) years, and a check of citizenship/residency, for each individual performing services under the Contract. Contractor shall complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee. Within three (3) days of completion, Contractor shall process the new employee through E-Verify to assist with verification of his/her status and the documents provided. The E-Verify is free of charge and can be located at www.uscis.gov/e-verify.

The criminal background check may be performed by a public or private entity and is done at the Contractor's expense, and shall be completed prior to any Contractor or subcontractor's employee providing services or accessing DHR data or Federal Tax Information (FTI) (including but not limited to electronic data and/or paper files). The CJIS background check shall cover a period of ten (10) years.

3.15.3 The CJIS criminal record check of each employee who will work on this Contract shall be reviewed by the Contractor for convictions of any of the following crimes described below, which shall constitute a bar to employment under the Contract if the conviction occurred within three (3) years from the date of the inquiry:
(a) child abuse;
(b) child neglect;
(c) spousal abuse;
(d) any other crime against children including possession and/or distribution of child pornography;
(e) a crime involving violence, including rape, sexual assault, homicide, or assault;
(f) a crime involving telecommunications and electronics; or
(g) crimes involving fraud and theft.

3.15.4 The Contractor shall provide a Criminal Background Check Affidavit (Attachment 16) for each employee, certifying to the Department that a background check has been performed. Prior to award, the Affidavits shall be submitted with the Proposals. After award, the Affidavits shall be submitted to the State Project Manager. Criminal background checks or reinvestigations must be conducted on all employees assigned to work under the Contract every three (3) years from the date of the previous background investigation.

3.15.5 If a prospective employee has been convicted of a criminal offense, including Probation Before Judgment, other than an offense listed in section 3.15.3 above, or if the conviction is more than three (3) years old, the Contractor shall make an initial individualized assessment of whether to hire the applicant. The Department reserves the right to reject any of Contractor's

employees or subcontractors that DHS determines, in its sole discretion, to be inconsistent with the performance and/or security requirements set forth in this Contract and DHS policy.

7. Add Internal Revenue Service requirements.

3.16 Safeguarding of Information from the United States Internal Revenue Service (IRS)

A. PERFORMANCE

The Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1. **All work shall be performed under the supervision of the Contractor or the Contractor's responsible employees.**

2. **The Contractor and the Contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.**

3. **Any Federal Tax Information (FTI) or return information (hereafter referred to as FTI, returns or return information) made available shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure to anyone other than an officer of employee of the Contractor is prohibited.**

4. **All returns and return information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.**

5. **The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.**

6. **Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the Department's Project Manager or designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the Department's Project Manager or designee with a statement containing the date of destruction, description of material destroyed, and the method used.**

7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

8. No work involving returns and return information furnished under this Contract shall be subcontracted without prior written approval of the IRS.

9. The Contractor shall maintain a list of employees authorized access. Such list will be provided to the Department and, upon request, to the IRS reviewing office.

10. The Department shall have the right to void the Contract if the Contractor fails to provide the safeguards described above.

B. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing solely by one designated person (from either DHS staff or the Contractor's staff, to be determined) that returns or return information disclosed to each officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as
$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by Internal Revenue Code (IRC) Sections 7213 and
7431 and set forth at 26 C.F.R. Part 301.6103(n)-1.

2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or

employee (United States for Federal Employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure, which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431 and set forth at 26 C.F.R. 301.6103(n)-1.

3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 United States Code (U.S.C.) 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

4. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors shall maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review.

As part of the certification and at least annually afterwards, Contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A. The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedures for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the Contractor shall sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements. See Attachment 15-1.

C. INSPECTION

The IRS and the Department, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with Contract safeguards. See Attachment 15

8. Revise Section 4.4.1.A Proposed Services as follows:

Executive Summary: A ~~one-page~~ **no more than 3-page** summary describing the Offeror's understanding of the TORFP Scope of Objectives (Section 3) and proposed solution.

9. Add Appendix **-4 MDTHINK Platform and Appendix -5 MDTHINK Infrastructure.**

Offerors are reminded that they must acknowledge receipt of all amendments issued against the TORFP in their cover letter. Should you require clarification of the information provided in this Amendment, please contact me via email at leah.hinson@maryland.gov or by telephone at (410) 238-1339.

Attachments:
1. Safeguarding Information from the United States Internal Revenue Service-ATTACHMENT 14
2. Annual Internal Revenue Service Employee Awareness- ATTACHMENT 15
3. Unauthorized Disclosure of Information- ATTACHMENT 15-1
4. Civil Damages and Unauthorized Inspection or Disclosure of Returns and
5. Return Information- ATTACHMENT 15-2
6. Reporting Improper Inspections or Disclosures- ATTACHMENT 15-3
7. Background Check Affidavit- ATTACHMENT 16
8. MDTHINK Platform - APPENDIX 4
9. MDTHINK Infrastructure – APPENDIX 5

By: Leah Hinson
Procurement Officer
Issued: September 12, 2017

ATTACHMENT 14 - SAFEGUARDING OF INFORMATION FROM THE UNITED STATES INTERNAL REVENUE SERVICE

A. PERFORMANCE

The Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1. All work shall be performed under the supervision of the Contractor or the Contractor's responsible employees.

2. The Contractor and the Contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

3. Any Federal Tax Information (FTI) or return information (hereafter referred to as FTI, returns or return information) made available shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure to anyone other than an officer of employee of the Contractor is prohibited.

4. All returns and return information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

5. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the Department's Project Manager or designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the Department's Project Manager or designee with a statement containing the date of destruction, description of material destroyed, and the method used.

7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

8. No work involving returns and return information furnished under this Contract shall be subcontracted without prior written approval of the IRS.

9. The Contractor shall maintain a list of employees authorized access. Such list will be provided to the Department and, upon request, to the IRS reviewing office.

10. The Department shall have the right to void the Contract if the Contractor fails to provide the safeguards described above.

B. **CRIMINAL/CIVIL SANCTIONS**

1. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing solely by one designated person (from either DHR staff or the Contractor's staff, to be determined) that returns or return information disclosed to each officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by Internal Revenue Code (IRC) Sections 7213 and 7431 and set forth at 26 C.F.R. Part 301.6103(n)-1.

2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee (United States for Federal Employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431 and set

forth at 26 C.F.R. 301.6103(n)-1.

3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 United States Code (U.S.C.) 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

4. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors shall maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A. The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedures for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the Contractor shall sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements. See **Attachment W**.

C. **INSPECTION**

The IRS and the Department, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

By signing this form, the Contractor certifies that it has read and understands the within security policy and procedures for safeguarding IRS information.

Company Name: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

ATTACHMENT 15– Annual Internal Revenue Service Employee Awareness

Solicitation Number: OTHS/MDTHK-18-009-S

Annual Internal Revenue Service (IRS) Employee Awareness Certification

- Employees must be advised at least annually of the provisions of Section 7213 of the Internal Revenue Code, which makes unauthorized disclosure of the Federal returns or return information a crime that may be punishable by a fine in any amount not exceeding $1,000.00, or imprisonment of not more than 1 year, or both, together with the cost of the prosecution. See Attachment 15-1.

- Employees who have access to Federal tax information must also be advised annually of the provisions of Section 7431 of the Internal Revenue Code which permits a taxpayer to bring suit for unauthorized disclosure in the United States district court. The taxpayer would be entitled to the greater of civil damages or the actual damages plus punitive damages in addition to the cost of the action. See Attachment 15-2.

- Employees are to be made aware that these civil and criminal penalties apply even if the unauthorized disclosures were made after their employment with the agency is terminated.

- The Department, as a part of their employee awareness training, is making it mandatory for all employees to be advised annually of the provisions of Title 07, Subtitle 01, Chapter 07, Section 10, (07.01.07.10) of the Code of Maryland Regulation (COMAR), which states, an intentional or grossly negligent disclosure of confidential information in violation of this chapter may be punishable by a fine of not more than $500.00, or by 90 days imprisonment, or both; and result in civil liability for damages.

- Employees shall execute an initial and annual training certification indicating that he or she understands the Department's security policy and procdures for safeguarding IRS information. The initial certification and recertifciation must be provided to the Departmnent.

THIS FORM IS TO BE SUBMITTED WITH WORK ORDER AND ANNUALLY THEREAFTER

I understand and agree to the above requirements.

_____

Contractor Name (Printed)

_____

Contractor Signature

_____

Date

ATTACHMENT 15-1 – UNAUTHORIZED DISCLOSURE OF INFORMATION

IRC SEC. 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES—It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in an manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

IRC SEC. 7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for

(A) any officer or employee of the United States, or
(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (l)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms "inspect" "return" and "return information" have respective meanings given such terms by section 6103(b).

ATTACHMENT 15-2 – CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION

(a) In general

(1) Inspection or Disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103 or in violation of section 6104 (c), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure-
(1) which results from good faith, but erroneous, interpretation of section 6103, or
(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of –

(1) the greater of –
(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or
(B) the sum of –
(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus
(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) Period for Bringing Action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of Unlawful Inspection and Disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of –

(1) paragraph (1) or (2) of section 7213 (a),

(2) section 7213A (a), or

(3) subparagraph (B) of section 1030(a)(2) of Title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return" and "return information" have the respective meanings given such terms by section 6103 (b).

(g) Extension to information obtained under section 3406

For purposes of this section –

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 6311 (e).

ATTACHMENT 15-3 – REPORTING INSPECTIONS AND DISCLOSURES

General

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the State Project Manager immediately, but, no later than 24 hours after identification of a possible issue involving FTI.

Notification Process

Concurrent to notifying the Department, the Contractor must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time the incident occurred
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data Incident report.

NOTE: Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Department as soon as it is available.

The Department will cooperate with Treasury Inspector General for Tax Administration (TIGTA) and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

ATTACHMENT 16 – CRIMINAL BACKGROUND CHECK AFFIDAVIT

Solicitation Number: OTHS/MDTHK-18-009-S

CRIMINAL BACKGROUND CHECK AFFIDAVIT

AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the TYPE TITLE HERE and the duly authorized representative of TYPE CONTRACTOR COMPLETE LEGAL NAME 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 TYPE CONTRACTOR COMPLETE LEGAL NAME has complied with Attachment 15 (Criminal Background Check Requirements).

I hereby affirm that the TYPE CONTRACTOR COMPLETE LEGAL NAME has provided the **Department of Human Services** with a summary of the security clearance results for all of the candidates that will be working on the **OTHS/MDTHK-18-009** and all of these candidates have successfully passed all of the background checks required. The Contractor hereby agrees to provide security clearance summary of results for any additional candidates at least seven (7) days prior to the date the candidate commences work on this Contract.

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.

Contractor

Typed Name

_____

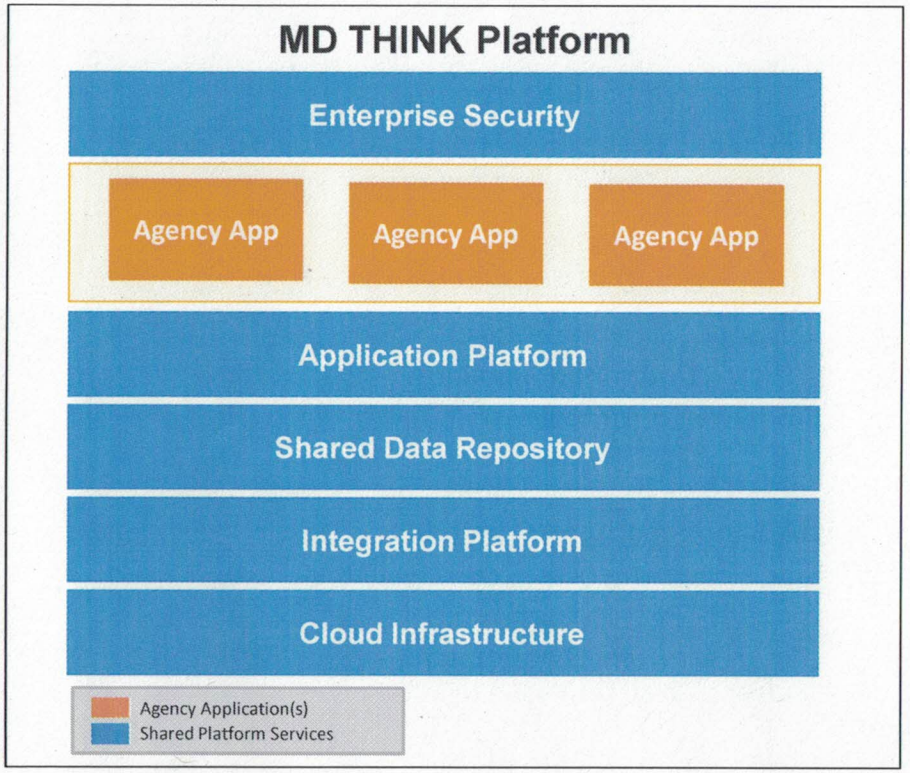
Signature

_____

Date

MD THINK Vision

MD THINK is a transformational, groundbreaking technology program that will modernize service delivery to the Marylanders



Platform Features

Enterprise Security

- Sophisticated platform meeting all Federal & State Requirements
- Uniform security policies and governance for all Apps

Cloud Infrastructure

- Highly scalable, yet affordable infrastructure
- Enables rapid setup with flexible configuration

Application Platform

- Full-featured application architecture providing all components required for developing sophisticated applications
- Ready to use, fully configurated application frameworks

Shared Data Repository & Analytics

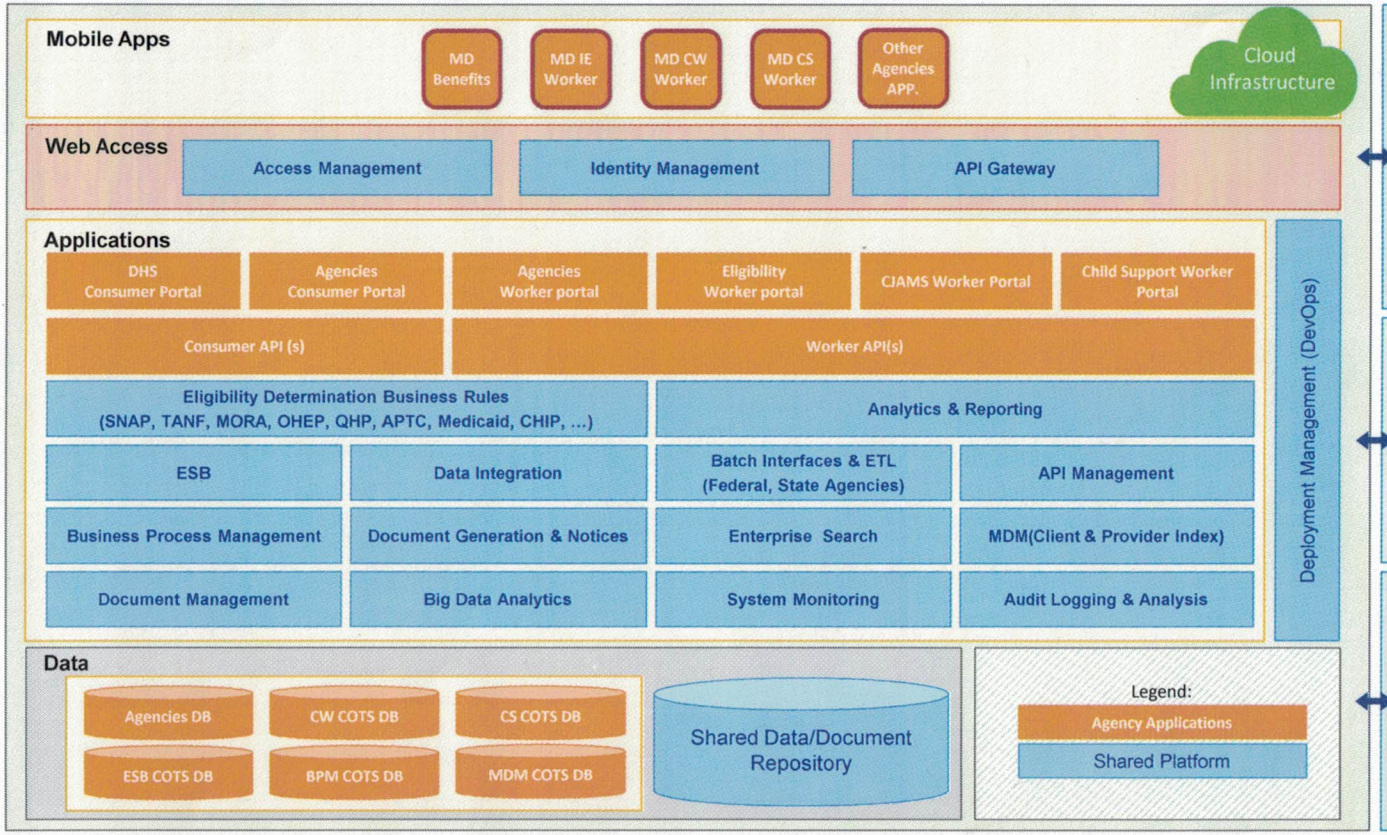
- Highly scalable, flexible and searchable shared data platform
- Provides, secure, role based access to cross-agency data

Integration Platform

- Ready-built interfaces with FDSH and State data systems
- Supports rapidly implementing additional interfaces

Application Architecture

The MD THINK Application Architecture will provide a groundbreaking shared platform supporting multiple Mission Specific Applications



Highlights

- Flexible, auto-scaling "pay as you go" **Cloud infrastructure**
- **Integrated web & mobile platform** for consumers and workers to provide user friendly and efficient access
- **APIs for all client and worker functions**, and for all business and technical areas to support plug and play architecture
- **Well defined Shared Platform** for supporting all Agency Apps, architected for additional agencies across the State
- **Shared Data Repository provides a 360 degree view and advanced analytics** across all programs and various product databases