AMENDMENT #1 – May 22, 2015

CATS+ - Task Order Request for Proposal K00B5400144

Compass Operations & Maintenance (O&M)

April 29, 2015

Ladies/Gentlemen:

This Amendment #1 is issued to amend and clarify certain information contained in the above referenced TORFP. All amendments are binding on all Offerors who respond to this TORFP. Specific parts of the TORFP have been amended as listed below. The following changes/additions are listed below; new language has been underlined and marked in bold (i.e., **word**) and language deleted has been marked with a strikeout (i.e., ~~word~~).

1) Revise page 4, Key Information Summary Sheet, as follows:

   Closing Date and Time: ~~5/26/2015~~ **6/8/2015** at 5:00 PM Local Time

2) Revise page 32-33, Section 2.9.1 OFFEROR'S COMPANY MINIMUM QUALIFICATIONS, as follows:

   Only those Master Contractors that fully meet all minimum qualifications criteria shall be eligible for TORFP proposal evaluation. The Master Contractor's proposal and references will be used to verify minimum qualifications.

   Only Master Contractor qualifications may be used to demonstrate meeting company minimum qualifications.

   The Master Contractor's proposal shall demonstrate meeting the following minimum requirements:

   A. At least ~~three (3)~~ **two (2)** years of demonstrated experience providing application hosting, helpdesk, and software development services to U.S. based commercial or government entities with at least ~~3,000~~ **1,000** users. **Demonstrated experience must be in the past five years.**

3) Revise page 12, Section 1.20 DEFINITIONS, System as follows:

   All services and activities necessary to fully support the Compass system as an Information System, described as services and/or products in this TORFP. This definition of System includes all System Source Materials developed as a result of this Task Order.

All Upgrades and regulatory updates shall be ~~provided at no additional cost to the State~~ **handled through the monthly O&M or time and materials work order process contained in this TORFP**.

4) Revise page 18, Section 2.6.1, TRANSITION-IN REQUIREMENTS, Requirement 2.6.1.14, as follows:

ID #	Transition-In Requirements	Associated Deliverable ID # from Section 2.8.4 below as applicable
2.6.1.14	The TO Contractor shall perform an initial scan of the operating system (OS) utilizing the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIGs) methodology and shall bring the OS and any other system and environment components into compliance.	***Deliverable 2.8.4.15 – System Compliance Scan***

5) Amend page 31, Section 2.8.4, DELIVERABLE DESCRIPTIONS, between Deliverables 2.8.4.7 and 2.8.4.8, as follows:

ID #	Deliverable Description	Acceptance Criteria	Due Date / Frequency
2.8.4.15	**System Compliance Scan**	**TO Contractor shall provide DNR a scan proving the OS and any other system and environment components are in compliance with the DISA STIGs.**	**NTP + 60 Calendar Days**

End Amendment #1

Issued by Jonathan Manley
Department of Natural Resources

MARYLAND
DEPARTMENT OF
NATURAL RESOURCES

Larry Hogan, *Governor*
Boyd K. Rutherford, *Lt. Governor*
Mark J. Belton, *Secretary*
Frank W. Dawson, III, *Deputy Secretary*

AMENDMENT #2 – June 3, 2015

CATS+ - Task Order Request for Proposal K00B5400144

Compass Operations & Maintenance (O&M)

April 29, 2015

Ladies/Gentlemen:

This Amendment #2 is issued to amend and clarify certain information contained in the above referenced TORFP. All amendments are binding on all Offerors who respond to this TORFP. Specific parts of the TORFP have been amended as listed below. The following changes/additions are listed below; new language has been underlined and marked in bold (i.e., **word**) and language deleted has been marked with a strikeout (i.e., ~~word~~).

1) Amend page 11, Section 1.20 DEFINITIONS, as follows:

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's 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.**
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.**

2) Revise page 36, Section 2.14 SOC 2 Type 2 AUDIT, as follows:

2.14.1 ~~In the event that a SOC 2 Type II Audit Report is required during the course of this Contract, DNR intends to initiate a SOC 2 Type II Audit by following the provisions in Right To Audit, as listed in Section 2.15.10. The scope of the SOC 2 Type II Audit, if needed, will include any Subcontractors providing services in support of this Contract that have access to Sensitive Data.~~ **This clause applies to the TO Contractor and Subcontractors who host the implemented Compass System for the State. The TO Contractor and/or Subcontractors who provide services that handle Sensitive Data (see definition of Handle Data in Section 1.20) for the Compass System must also comply with this clause, assuming the TO Contractor and/or Subcontractor receives copies of any data for use in providing services, including any system and/or user acceptance testing of the new System and any provided data that contains Sensitive Data.**

2.14.2 ~~Where possible, DNR will provide advance notice to the Contractor and any Subcontractors.~~ **The TO Contractor shall have an annual audit performed by an independent audit firm of the TO Contractor and/or Subcontractors' handling of Sensitive Data and/or the DNR's critical functions, which is identified as system hosting, operations and maintenance support and development, and shall address all areas relating to information technology security and operational processes. These services provided by the TO Contractor and/or Subcontractors that shall be covered by the audit will collectively be referred to as the "Information Functions and/or Processes." Such audits shall be performed in accordance with audit guidance: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the DNR, to assess the security of outsourced client functions or data (collectively, the "Guidance") as follows:**

2.14.2.1 The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the "SOC 2 Report"). The initial SOC 2 Report audit shall be scheduled and completed within a timeframe to be specified by the State and submitted to the TO Manager. All subsequent SOC 2 audits that are arranged after this initial audit shall be performed on an annual basis within a timeframe to be specified by the State and shall be submitted to the TO Manager.

2.14.2.2 The SOC 2 Report shall report on the description of the TO Contractor and/or Subcontractors' system and controls and the suitability of the design and operating effectiveness of controls over the Information Functions and/or Processes relevant to the following trust principles: Security, Availability, and Confidentiality as defined in the aforementioned Guidance. The SOC 2 Report should also report on the suitability of the design and operating effectiveness of controls of the Information Functions and/or Processes to meet the requirements of the TO Agreement, specifically the security requirements identified in Section 2.16.

2.14.2.3 The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Confidentiality, Processing Integrity, and Privacy) to accommodate any changes to the TO Contractor's and/or Subcontractors' environment since the last SOC 2 Report. Such changes may include but are not limited to the addition of Information Functions and/or Processes through change orders or Work Orders under the TO Agreement; or, due to changes in information technology or operational infrastructure implemented by the TO Contractor and/or Subcontractors. The TO Contractor and/or Subcontractors shall ensure that the audit scope of each year's SOC 2 Report engagement shall accommodate these changes by including in SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the TO Agreement.

2.14.2.4 The scope of the SOC 2 Report shall include work performed by any Subcontractors that provide essential support to the TO Contractor and/or essential support to the Information Functions and/or Processes provided to the DNR under the TO Agreement.

The TO Contractor shall ensure the audit includes all of these Subcontractor(s) in the performance of the SOC 2 Report.

2.14.2.5 All SOC 2 Reports, including those of the TO Contractor and/or Subcontractor, shall be performed at no additional expense to the DNR.

2.14.2.6 The TO Contractor and/or Subcontractors shall promptly provide a complete copy of the final SOC 2 Report to the TO Manager upon completion of each annual SOC 2 Report engagement.

2.14.2.7 The TO Contractor shall provide to the TO Manager, within 30 calendar days of the issuance of each annual final SOC 2 Report, a documented corrective action plan which addresses each audit finding or exception contained in the SOC 2 Report. The corrective action plan shall identify in detail the remedial action to be taken by the TO Contractor and/or Subcontractors along with the date(s) when each remedial action is to be implemented.

2.14.2.8 If the TO Contractor and/or Subcontractors currently have an annual information security assessment performed that includes the operations, systems, and repositories of the products/services being provided to the DNR under the TO Agreement, and if that assessment generally conforms to the content and objective of the Guidance, the DNR will determine in consultation with appropriate State government technology and audit authorities whether the TO Contractor and/or Subcontractors' current information security assessments are acceptable in lieu of the SOC 2 Report.

2.14.2.9 **If the TO Contractor and/or Subcontractors fail during the TO Agreement term to obtain an annual SOC 2 Report by the date specified in 2.14.2.1, the DNR shall have the right to retain an independent audit firm to perform an audit engagement of a SOC 2 Report of the Information Functions and/or Processes being provided by the TO Contractor and/or Subcontractors. The TO Contractor and/or Subcontractors agree to allow the independent audit firm to access its facility/ies for purposes of conducting this audit engagement(s), and will provide the support and cooperation to the independent audit firm that is required to perform the SOC 2 Report. The DNR will invoice the TO Contractor for the expense of the SOC 2 Report(s), or deduct the cost from future payments to the TO Contractor.**

3) Amend page 40, Section 2, SCOPE OF WORK, as follows:

2.18 **INSURANCE**

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).

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. The recommended awardee must provide a certificate(s) of insurance with the prescribed coverages, limits and requirements set forth in this Section 2.18.1 "Cyber Security / Data Breach Insurance" within five (5) Business Days from notice of recommended award. During the period of

performance for multi-year contracts the TO Contractor shall update certificates of insurance annually, or as otherwise directed by the TO Contract Manager.

2.18.1. CYBER SECURITY / DATA BREACH INSURANCE

In addition to the insurance specified in the Master Contract Section 2.7, TO Contractor shall maintain Cyber Security / Data Breach Insurance in the amount of ten million dollars ($10,000,000) per occurrence. The coverage must be valid in at all locations where work is performed or data or other information concerning the State's claimants and/or employers is processed or stored.

4) Amend page 45, Section 3.4.1.K, as follows:

c. Affirmative statement from the Offeror that an annual audit complying with Section 2.14 will be performed.

5) Revise page 39, 2.16.2 Data Protection, B.3, as follows:

~~Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration. Data encryption shall be applied to State data in transit over networks, to State data when archived for backup purposes, and, where possible, State data at rest. Encryption algorithms which are utilized for this purpose must comply with current National Institute of Standards and Technology recommendations contained in NIST Special Publication 800-131a (csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf).~~**Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration. Data encryption should be applied to State data in transit over networks and, where possible, State data at rest within the system; as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.**
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

6) Revise page 4, Key Information Summary Sheet, as follows:

Closing Date and Time: ~~5/26/2015~~ **6/15/2015** at 5:00 PM Local Time

End Amendment #2

Issued by Jonathan Manley
Department of Natural Resources