
ATTACHMENT 3

**CYBERSECURITY- PRIVACY REQUIREMENTS FOR UNCLASSIFIED
INFORMATION TECHNOLOGY (IT) RESOURCES**

(September 2017)

-
- (a) Required Policies and Regulations - The Contractor shall comply with all prevailing Department of Transportation (DOT), Federal Motor Carriers Safety Administration (FMCSA), and Federal IT Security standards, policies, and reporting requirements, including:
- (1) Federal Information Security Modernization Act (FISMA) of 2014
 - (2) Clinger-Cohen Act of 1996 also known as the “Information Technology Management Reform Act of 1996.”
 - (3) Privacy Act of 1974 (5 U.S.C. § 552a)
 - (4) Homeland Security Presidential Directive (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors”, August 27, 2004
 - (5) Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources”, and Appendix III, “Security of Federal Automated Information Systems”, as amended.
 - (6) OMB Memorandum M-03-22 – OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
 - (7) OMB Memorandum M-04-04, “E-Authentication Guidance.”
 - (8) OMB Memorandum M-05-04, “Policies for Federal Agency Public Websites (December 17, 2004) Best Practices”
 - (9) OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors”
 - (10) OMB Memorandum M-06-15, “Safeguarding Personally Identifiable Information (May 22, 2006)”
 - (11) OMB Memorandum M-06-16, “Protection of Sensitive Agency Information”
 - (12) OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)”
 - (13) OMB Memorandum M-06-20, “FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”

-
- (14) OMB Memorandum M-07-16, "Safeguarding Against & Responding to Breach of Personally Identifiable Information"
 - (15) OMB Memorandum M-07-19, "Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management "
 - (16) OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC)"
 - (17) OMB Memorandum M-08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)"
 - (18) OMB Memorandum M-08-23, "Securing the Federal Government's Domain Name System Infrastructure"
 - (19) OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)"
 - (20) OMB M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
 - (21) Federal Information Processing Standards (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems."
 - (22) FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems."
 - (23) FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."
 - (24) FIPS PUB 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors."
 - (25) Federal Enterprise Architecture - Security and Privacy Profile (FEA-SPP) version 3 May 5, 2009
 - (26) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing Security Plans for Federal Information Systems"
 - (27) NIST SP 800-28, "Guidelines on Active Content and Mobile Code"
 - (28) NIST Special Publication 800-30, "Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems"

-
- (29) NIST SP 800-32, “Introduction to Public Key Technology and the Federal PKI Infrastructure”
 - (30) NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems”
 - (31) NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
 - (32) NIST SP 800-40, “Creating a Patch and Vulnerability Management Program”
 - (33) NIST SP 800-41, “Guidelines on Firewalls and Firewall Policy”
 - (34) NIST SP 800-44, “Guidelines on Securing Public Web Servers”
 - (35) NIST SP 800-46, “Guide to Enterprise Telework and Remote Access Security”
 - (36) NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”
 - (37) NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”
 - (38) NIST SP 800-53A, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans”
 - (39) NIST SP 800-57 (Parts 1-3), “Recommendation for Key Management”
 - (40) NIST SP 800-60 Vol 1&2), “Guide for Mapping Types of Information and Information Systems to Security Categories”
 - (41) NIST SP 800-61, “Computer Security Incident Handling Guide”
 - (42) NIST SP 800-63-2, “Electronic Authentication Guidance”
 - (43) NIST SP 800-64, “Security Considerations in the System Development Life Cycle”
 - (44) NIST SP 800-73-4, “Interfaces for Personal Identity Verifications (4 Parts).”
 - (45) NIST SP 800-77, “Guide to IPSec VPNs”
 - (46) NIST SP 800-78-4, “Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)”
 - (47) NIST SP 800-79-2, “Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)”

-
- (48) NIST SP 800-81, “Secure Domain Name System (DNS) Deployment Guide”
 - (49) NIST SP 800-83, “Guide to Malware Incident Prevention and Handling for Desktops and Laptops”
 - (50) NIST SP 800-85A-4, “PIV Card Application and Middleware Interface Test Guidelines (SP800-73-4 Compliance)”
 - (51) NIST SP 800-85 B, “PIV Data Model Test Guidelines”
 - (52) NIST SP 800-87, “Codes for Identification of Federal and Federally-Assisted Organizations”
 - (53) NIST SP 800-88, Guidelines for Media Sanitization”
 - (54) NIST SP 800-92, “Guide to Computer Security Log Management”
 - (55) NIST SP 800-96, “Guide to Secure Web Services”
 - (56) NIST SP 800-96, “PIV Card to Reader Interoperability Guidelines”
 - (57) NIST SP 800-111, “Guide to Storage Encryption Technologies for End User Devices”
 - (58) NIST SP 800-115, “Technical Guide to Information Security Testing and Assessment”
 - (59) NIST SP 800-116, “A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)”
 - (60) NIST SP 800-119, “Guidelines for the Secure Deployment of IPv6”
 - (61) NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”
 - (62) NIST SP 800-123, “Guide to General Server Security”
 - (63) NIST SP 800-125, “Guide to Security for Full Virtualization Technologies”
 - (64) NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
 - (65) NIST SP 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”

-
- (66) C.F.R. Part 5 Subpart C (5 C.F.R 930.301), "Information Security Responsibilities for Employees Who Manage Or Use Federal Information Systems: Information systems security awareness training program"
 - (67) Center of Internet Security (CIS) Benchmarks/Guidelines (Level 1 for internal systems and Level 1&2 for external facing systems)
 - (68) National Vulnerability Database Guidelines
 - (69) Confidential Information Protection and Statistical Efficiency Act of 2002 (Pub. L. No. 107-347, Title V, Dec. 17, 2002, 116 Stat. 2962)
 - (70) Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)
 - (71) Federal Records Act of 1950 (44 U.S.C. Ch 31)
 - (72) Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.)
 - (73) DOT Order 1351.37, "Departmental Cybersecurity Policy"
 - (74) DOT Departmental Cybersecurity Compendium "Supplement to DOT Order 1351.37 Departmental Cybersecurity Policy"
 - (75) DOT Information Technology and Information Assurance Policy: Implementation of DOT's Protection of Sensitive Personally Identifiable Information (Spii)
 - (76) DOT Security Authorization and Continuous Monitoring Guide
 - (77) DOT Weakness Management Guide
 - (78) DOT Automated Continuous Monitoring Guide
- (b) Applicability - The Contractor shall be responsible for Information Technology security for all systems connected to a FMCSA network or operated by the Contractor for FMCSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to FMCSA information that supports the mission of FMCSA. The term information technology, as used in this clause, means any equipment or interconnected system or subsystem of equipment, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general supports systems as defined by OMB Circular A-130.

-
- (c) Security Categorization - In accordance with FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems", FMCSA has determined that the security category of the information or information system under this contract is MODERATE. The Contractor shall tailor an appropriate set of baseline security requirements as outlined in NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems", and the Center of Internet Security (CIS) guidelines (Level 1 for internal systems and Level 1&2 for external facing systems).
- (d) IT Security Requirements and Documentation – All covered Contractor systems/applications must have a valid security assessment and authorization signed and approved by the Government in accordance with the DOT Departmental Cybersecurity Compendium, before going into operation and/or processing FMCSA information. While operational, the system must be re-assessed on an annual basis to ensure the system maintains a valid authorization, signed and approved by the Government. The Contractor shall prepare and submit documents necessary to support security assessment activities and authorization of any covered systems no less than 90 days prior to initial operation and processing of FMCSA information. These documents shall be updated on an annual basis. The security assessment and authorization documents listed below shall be consistent in form and content with the approved FMCSA format. In accordance with the DOT Security Authorization and Continuous Monitoring Performance Guide, approximately one third of the security controls for each Information system must be assessed yearly. The exact security controls to be assessed can be found in the system's approved Continuous Monitoring Plan. In the event there is a significant change to the system's security posture the entire security authorization must be reassessed in accordance with NIST SP 800-37, and the DOT Departmental Cybersecurity Compendium. The Contractor shall provide the necessary support to ensure the security assessment is completed prior to the system authorization expiration date.

In support of the security assessment and authorization, the Contractor shall submit to the COR the following documents:

- (1) System Development Life Cycle - The Contractor shall prepare and provide System Development Life Cycle consistent in form and content with NIST SP 800-64, "Security Considerations in the System Development Life Cycle", and NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)" and any additional guidance contained in the DOT Departmental Cybersecurity Compendium.
- (2) Security Architecture Design Document - The Contractor shall prepare and provide Security Architecture Design Document consistent in form and content with NIST SP 800-64, "Security Considerations in the System Development Life Cycle". The Security Architecture Design Document is a schematic of security integration providing details on where, within the system, security is implemented and shared. Security architectures should be graphically depicted and detailed to the extent the reader can

see where the core security controls are applied and how. The Security Architecture Design Document shall be updated on an annual basis to reflect any changes.

- (3) Configuration Management Plan – The Contractor shall prepare and provide Configuration Management Plan consistent in form and content with NIST SP800-128, “Guide for Security-Focused Configuration Management of Information Systems” and NIST SP 800-53, “Recommended Security Controls for Federal Information Systems” control CM-9. The Configuration Management Plan for the information system should:
 - i) Address roles, responsibilities, and configuration management processes and procedures;
 - ii) Define the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
 - iii) Establish the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
- (4) System Security Plan (SSP) – Prepare consistent in form and content with NIST SP 800-18, “Guide for Developing Security Plans for Federal Information Systems.” The SSP shall include as appendices required policies and procedures across 18 control families mandated per FIPS 200, Rules of Behavior, and Interconnection Agreements, consistent with NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.” The SSP shall also address the controls specified in NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” and NIST SP 800-53, “Recommended Security Controls for Federal Information Systems” and the DOT Departmental Cybersecurity Compendium. The SSP should describe the security controls in place or planned for meeting those requirements. The SSP shall be updated on an annual basis.
- (5) Security Assessment Plan and Report - The Contractor shall support the independent third-party assessor in the creation of the Security Assessment Plan (SAP) in support of the annual security authorization process for the delivered information system consistent with NIST 800-53, “Recommended Security Controls for Federal Information Systems” control SA-11.
- (6) Information System Documentation – The Contractor shall:
 - i) create and provide documentation for the information system that describes:
 - Secure configuration, installation, and operation of the information system;
 - Effective use and maintenance of security features/functions; and
 - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions
 - ii) create and provide user documentation for the information system that describes:
 - User-accessible security features/functions and how to effectively use those security features/functions;

-
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
 - User responsibilities in maintaining the security of the information and information system; and
 - Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
- (7) FIPS 199 Assessment – The FIPS 199 assessment shall identify all information types as well as the “high water mark,” as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.
- (8) Contingency Plan (including Disaster Recovery Plan) – Prepared consistent in form and content with NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems”, and any additional guidance contained in the DOT Departmental Cybersecurity Compendium. Consistent with NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems”. The Contractor shall also provide an annual Independent Penetration Test Report, documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. The Contingency Plan shall be updated on annual basis.
- (9) Business Impact Assessment - As part of the Contingency Plan, the Contractor shall perform a Business Impact Assessment prior to the system delivery, or when significant changes are introduced. The Business Impact Assessment shall be updated on a yearly basis.
- (e) Security Assessment and Authorization Activities –The Contractor shall allow an FMCSA designated independent third party assessor, also known as a 3PAO, to conduct the initial and subsequent annual security assessment and authorization activities to include control reviews in accordance with NIST SP 800-53, “Recommended Security Controls for Federal Information Systems” and NIST SP 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems” and the DOT Departmental Cybersecurity Compendium. In accordance with NIST guidance, the third party contractor shall be an impartial assessor of the system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Review activities include, but are not limited to, operating system vulnerability scanning, web application scanning, database scanning, and integrity verification scans of applicable systems that support the processing, transportation, storage, or security of FMCSA information. This includes the general support system infrastructure.

-
- (1) Identified gaps between required NIST 800-53, “Recommended Security Controls for Federal Information Systems” controls and the Contractor’s implementation, as documented in the Security Assessment/Risk Assessment report, shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) completed in accordance with DOT Departmental Cybersecurity Compendium. Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
 - (2) The contractor is responsible for mitigating all security risks found during the initial and annual security assessment and authorization. All critical and high vulnerabilities must be mitigated immediately. During continuous monitoring activities, the following guidance applies: Remediate within 7 days for critical, 30 days for high, 60 days for medium, 90 days for lows and at the discretion of the Authorizing Official for informational vulnerabilities.
 - (3) The Contractor shall provide support for an Independent Security Assessment/Risk Assessment in accordance with NIST SP 800-137 - “Information Security Continuous Monitoring for Federal Information Systems and Organizations” and the DOT Departmental Cybersecurity Compendium for the annual security assessment and authorization activities.
- (f) Annual Security Controls Assessment - Information systems must be assessed yearly or whenever there is a significant change to the system’s security posture in accordance with NIST SP 800-37, and the DOT Departmental Cybersecurity Compendium. The annual security controls assessment testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a 3-year period, all DOT Minimum Security Controls applicable to a system or application shall be tested. This means a subset (no less than one-third [1 / 3]) of the minimum security controls shall be tested each year so that all security controls are tested during a 3-year period. In an effort to standardize testing and results summarization, a 3-year rotation of control families was established by DOT. As control families are added or removed, DOT CIO reserves the right to change the controls that must be tested each year. To fulfill the annual FMCSA validation obligation, the annual security control assessment shall be conducted by an FMCSA impartial independent agent or team. It is the responsibility of FMCSA to procure the services of an independent third party assessor to ensure impartiality from the contractor managing the accredited system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of DOT Minimum Security Controls effectiveness. All management-directed and independent testing conducted within 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., annual security control assessment) testing. Upon successful completion of the Independent Security Assessment/ Risk Assessment, FMCSA (in coordination with the information system Program Manager and

Information System Security Manager (ISSM)) will communicate an authorization decision to the Authorizing Official to accept or deny assigned risks.

- (g) Continuous Monitoring - The Contractor shall facilitate a consistent approach to managing security risks for FMCSA IT systems in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 (as amended), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, National Institute of Standards and Technology Special Publication 800-137 (as amended), Information Security Continuous Monitoring for Federal Information Systems and Organizations, DOT Security Authorization and Continuous Monitoring Performance Guide, and FMCSA Continuous Monitoring Plan. The Contractor shall provide oversight and monitoring of security controls for managing all systems and software operated by the Contractor. The Contractor shall develop methods for advising and auditing operational and business practices so as to ensure due diligence and provide adequate security for the systems under their control or responsibility.

The Contractor shall report on all asset within the FMCSA system accreditation boundary on an ongoing basis and inform the COR and ISSM when changes occur that may impact the security of the system.

The Contractor shall perform review activities to include, but are not limited to, weekly operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of FMCSA information using the relevant tools as required and directed by the ISSM, identify deficiencies and make recommendations for remedies to the ISSM. The Contractor shall develop the reporting processes necessary to provide FMCSA ISSM and Management with real-time visibility and scoring of the security posture and its assets.

For in-house developed, third-party procured web or application software, and static code scanning software in accordance with the DOT Cyber Compendium Risk Assessment Policy RA-5, the contractor shall be responsible for testing coding errors prior to deployment using automated static code analysis software. If source code is not available, the contractor shall test the compiled code using a static binary analysis tools. A static code scan shall be conducted whenever there is a change to the source code or as part of the annual system security assessment.

The Contractor shall provide the relevant tools necessary for the execution of system security continuous monitoring to ensure completion of the above tasks.

- (h) Contract Compliance - Upon approval by the Government, the Systems Security Plan, Configuration Management Plan, Incident Response Plan, Software Development Life Cycle Methodology, FIPS 199 Assessment, and Contingency Plan, including any required updates, shall be incorporated into the contract file as compliance documents. The Level of Effort for

the security assessment and authorization is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization.

- (i) Availability of Documents and Access - The Contractor shall provide FMCSA (or FMCSA independent third party assessor) access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out physical security site assessments, investigations, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of FMCSA information or to the functions of information technology operated on behalf of FMCSA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of FMCSA information, stored and/or processed, either by information systems in direct support of the Contractor or that are incidental to the contract.
- (j) Annual Deliverables: The Contractor shall provide, on an annual basis, the following documents to the contracting officer:
 - (1) Updated Security Assessment and Authorization documentation - Including the System Security Plan, Plan of Action and Milestones, Business Impact Assessment, and Contingency Plan.
 - i. System Security Plan - Reference: NIST 800-53, "Recommended Security Controls for Federal Information Systems" control PL-2 - Contractor shall:
 - 1. Develop a security plan for the information system that:
 - Is consistent with the organization's enterprise architecture;
 - Explicitly defines the authorization boundary for the system;
 - Describes the operational context of the information system in terms of missions and business processes;
 - Provides the security categorization of the information system including supporting rationale;
 - Describes the operational environment for the information system;
 - Describes relationships with or connections to other information systems;
 - Provides an overview of the security requirements for the system;
 - Describes the security controls in place or plans for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
 - Is reviewed and approved by the Authorizing Official or designated representative prior to plan implementation;
 - 2. Review the security plan for the information system annually; and

-
- 3. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
 - 4. The System Security Plan must be in accordance with NIST 800-18, "Guide for Developing Security Plans"
 - ii. Contingency Plan Test and Disaster Recovery Plan Test - Reference: NIST 800-53, "Recommended Security Controls for Federal Information Systems" control CP-2 – The Contractor shall provide an annual update to the contingency plan completed in accordance with NIST 800-34, "Contingency Planning Guide." The Contractor shall perform a yearly tabletop Contingency Plan Test and provide a report detailing the results of the test to the FMCSA ISSM and COR.
 - iii. Disaster Recovery Test - The Contractor shall also perform a full functional Disaster Recovery Test every three years and provide a report (Deliverable XX) detailing the results of the test to the FMCSA ISSM and COR. For any new systems, the Contractor shall ensure the Disaster Recovery Test is performed prior to implementation. The contractor shall train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.
 - iv. FIPS 199 Assessment – The Contractor shall provide an update to the FIPS 199 assessment which shall identify all information types as well as the "high water mark," as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.
 - (2) User Authorization Review Documents - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" controls AC-2 – The Contractor shall provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
 - (3) Separation of Duties Matrix - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control AC-5 - The Contractor shall develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes.
 - (4) Information Security Awareness and Training Records - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control AT-4 –The Contractor shall ensure that employees receive security awareness (AT-2) and role-based information security technical training (AT-3) and shall provide documentation of

this training to FMCSA. AT-2 requires basic security awareness training for FMCSA employees and contractors that support the operation of the Contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

- (5) System(s) Baseline Configuration Standard Document - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control CM-2 – the Contractor shall provide a well-defined, documented, and up-to-date a current baseline configuration of the information system.
- (6) System Configuration Settings - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control CM-6 – The Contractor shall establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system; and identify and document exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements. Systems should be configured in agreement with NIST guidelines at the NIST Checklist website (checklists.nist.gov) and the Center for Internet Security (CIS) guidelines (Level 1 - for internal information systems), Level 1&2 – for external facing information systems), and the National Vulnerability Database Guidelines, unless a waiver is granted by the FMCSA CIO/ISSO.
- (7) Configuration Management Plan - Reference: NIST SP800-128, "Guide for Security-Focused Configuration Management of Information Systems" and NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control CM-9 – The Contractor shall develop and provide an annual update to the Configuration Management Plan for the information system that:
 - i. Addresses roles, responsibilities, and configuration management processes and procedures;
 - ii. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
 - iii. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
- (8) Incident Response Plan - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control IR-8 - The Contractor shall:
 - i. Develop an incident response plan that:
 - Provides the organization with a roadmap for implementing its incident response capability;

-
- Describes the structure and organization of the incident response capability;
 - Provides a high-level approach for how the incident response capability fits into the overall organization;
 - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
 - Defines reportable incidents;
 - Provides metrics for measuring the incident response capability within the organization;
 - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
 - Is reviewed and approved by designated officials within the organization;
- ii. Review the plan annually;
 - iii. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
 - iv. Integrate with and incorporate guidance and procedures from the DOT CSIRC to ensure effective detection, reporting and response.
 - v. The Incident Response Plan must be in accordance with NIST 800-61, "Computer Security Incident Handling Guide"
- (9) Incident Response Test Report - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control IR-3 - The Contractor shall provide an incident response test report documenting results of incident reporting test/exercise in accordance with the DOT Departmental Cybersecurity Compendium.
- (10) Results of Physical Security User Security Assessment and Authorization Review - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control PE-2 – The Contractor shall provide the results of annual reviews and validations of physical access authorizations to facilities supporting the Contractor system to ensure the continued need for physical access.
- (11) Results of Review of Physical Visitor Access Records - Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control PE-8 – The Contractor shall provide the results of annual reviews and validations of visitor access records to ensure the accuracy and fidelity of collected data.
- (12) Maintenance Records – Reference: NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" control MA-2(2) – The Contractor shall provide up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

(13) Information System Interconnection Agreements - Reference: NIST SP 800-53, “Recommended Security Controls for Federal Information Systems” control CA-3 – The Contractor shall provide updated Interconnection Security Agreements (ISA) and supporting Memorandum of Agreement/Understanding (MOA/U), completed in accordance with NIST SP 800-47, “Security Guide for Connecting Information Technology Systems”, for existing and new interconnections. Per NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems” an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. Interconnections agreements shall be submitted as appendices to the System Security Plan.

(14) Rules of Behavior - Reference: NIST 800-53, “Recommended Security Controls for Federal Information Systems” control PL-4 – The Contractor shall a. establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

(15) Additional Deliverables:

- i. Monthly training records in accordance with FMCSA IT Security Training Policy
- ii. Monthly POAM and vulnerability updates in accordance with FMCSA IT Security POAM and Vulnerability Management Policy
- iii. Monthly scan summary and reports in accordance with FMCSA IT Security Vulnerability Management Policy
- iv. Respond to datacall and security advisories in accordance with FMCSA IT Security Advisory Policy

(k) Controlled Unclassified Information - All deliverables under this section shall be labeled according to the sensitivity of the information. FOR OFFICIAL USE ONLY (FOUO), Sensitive Security Information (SSI), and/or other designations as directed by FMCSA shall be applied to paper and electronic documents. External transmission/dissemination of sensitive unclassified information to or from a FMCSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, “Security requirements for Cryptographic Modules.” Handling, storage, processing, transmitting and discussing of Controlled Unclassified Information shall be in accordance with FMCSA guidance in order to prevent the release of such information to persons not authorized by FMCSA to have access to the information.

(l) HSPD-12 / Identity, Credential and Access Management Requirements – The Contractor shall ensure, at a minimum, that all systems that it develops for or operates on behalf of the Government support the use of Personal Identity Verification (PIV) smart cards, and PIV

interoperable (PIV-I) smart cards as appropriate, for authentication and access to those systems, for the digital signature of documents and workflows, and for the encryption of documents and information, in accordance with NIST PUB 201 and related special publications. **When explicitly required, or by September 30, 2012, whichever occurs sooner, the Contractor shall ensure that all systems it develops for or operates on behalf of the Government meet applicable DOT/FMCSA policy requirements for identity, credential and access management (ICAM) and require the use of a PIV card or PIV-I for authentication, access, digital signature, and encryption.** The Contractor shall ensure that services and products it purchases involving facility or system access control are on the current FIPS 201 Approved Products List which can be found on <http://www.idmanagement.gov/>.

- (m) **Internet Protocol Version 6 (IPV6) Mandate**- The contractor shall ensure that all applicable systems that it develops for or operates on behalf of the Government are compatible with IPV6. The contactor must perform testing to validate IPv6 compatibility. IPV6 validation tests must include the test date, method of testing used the validate IPV6 compatibility. Test results must be submitted to FMCSA ISSO for validation.
- (n) **Domain Name System Security Extension (DNSSEC) Mandate**- The contractor shall implement DNSSEC on all second level DNS servers to prevent the pirating of government domain names. The contractor must validate DNSSEC compliance to FMCSA ISSM.
- (o) **Trusted Internet Connection (TIC)** – The contractor shall ensure that all applicable systems that it develops for or operates on behalf of the Government are compliant with National Security Presidential Directive 54 and Homeland Security Presidential Directive 23.
- (p) **Federal Desktop Core Configuration/US Government Configuration Baseline** - The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC)/US Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved FDCC/USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default “program files” directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with FDCC/USGCB Scanner capability to certify their products operate correctly with FDCC/USGCB configurations and do not alter FDCC/USGCB settings.
- (q) **Privacy Threshold Analysis (PTA)** - The Contractor shall provide support to FMCSA in developing Privacy Threshold Analysis.

-
- (r) Privacy Impact Assessment (PIA) - The Contractor shall provide support to FMCSA in developing Privacy Impact Assessments in accordance with Section 208 of the e-Government Act of 2002.
- (s) System of Record Notice (SORN) - The Contractor shall provide support to FMCSA in developing System of Record Notices (SORN) in accordance with the Privacy Act of 1974.
- (t) System Access Notice - The Contractor shall ensure that the following banners are displayed on all FMCSA systems (both public and private) operated by the Contractor prior to allowing authenticated access to the system(s):

“ATTENTION ATTENTION ATTENTION

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
 - You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
 - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

[click button: “I AGREE”]

- (u) Privacy Act Notifications - As prescribed in the Federal Acquisition Regulation (FAR) clause 24.104, if the system involves the design, development, or operation of a system of records on individuals, the Contractor shall implement requirements in FAR clause 52.224-1, “Privacy Act Notification” and FAR clause 52.224-2, “Privacy Act.” The Contractor shall ensure that the following banner is displayed on all FMCSA systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

“This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Individuals who violate privacy safeguards may be subject to disciplinary actions, a fine of up to \$5,000, or both.”

-
- (v) Non-Disclosure Agreements - The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
- (w) Non-Disclosure of Security Safeguards - In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following privacy and security safeguards: The Contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- (x) Security of Systems Handling Personally Identifiable Information and Privacy Incident Response
- (1) Definitions.
- “Breach” (may be used interchangeably with “Privacy Incident”) as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.
- “Personally Identifiable Information (PII)” as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.
- Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.
- “Sensitive Personally Identifiable Information (Sensitive PII)” as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information

that contains an individual's name or other unique identifier plus one or more of the following elements:

- i. Driver's license number, passport number, or truncated SSN (such as last 4 digits)
- ii. Date of birth (month, day, and year)
- iii. Citizenship or immigration status
- iv. Financial information such as account numbers or Electronic Funds Transfer Information
- v. Medical Information
- vi. System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

(2) Systems Access.

Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(3) Systems Security

In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements or any replacement publication and rules of conduct described in DOT Order 1351.37.

In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:

- i. Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
- ii. The contractor has developed and implemented a process to ensure that security and other applications software are kept current;

-
- iii. The contractors are responsible for implementing mechanisms to protect the integrity of the data by employing integrity verification tools;
 - iv. Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
 - v. When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DOT security requirements.
 - vi. The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
 - vii. Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
 - 1. Authorized and official use;
 - 2. Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
 - 3. Prohibition against access by unauthorized users and unauthorized use by authorized users; and
 - 4. Protection of Sensitive PII;
 - viii. All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DOT Order 1351.14 which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(4) Data Security

Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.

(5) Breach Response.

The contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COTR), and the FMCSA Privacy Officer (fmcsasecurity@dot.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

(6) Personally Identifiable Information Notification Requirement.

The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DOT Privacy incident handling guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

CONTRACT CLAUSES

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

<https://www.acquisition.gov/far/>.

- 52.203-13, Contractor Code of Business Ethics and Conduct
- 2.215-2, Audit and Records - Negotiation
- 52.239-1, Privacy or Security Safeguards
- 52.203-13, Contractor Code of Business Ethics and Conduct, which states that the contractor's internal control system shall provide for full cooperation with any Government agencies responsible for audits, investigations, or corrective actions. Full cooperation is defined as "disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Government auditors' and investigators' request for documents and access to employees with information."
- 52.215-2, Audit and Records—Negotiation, which states that the Comptroller General, an appropriate Inspector General, or an authorized representative of either, shall have access to and the right to examine any of the Contractor's or any subcontractor's records that pertain to and involve transactions relating to this contract or a subcontract hereunder; and interview any officer or employee regarding such transactions.
- 52.239-1, Privacy or Security Safeguards, which states that "To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases."

(a) Pass-Through of Security and Privacy Requirements to Subcontractors.

The contractor shall incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

(b) Federal Information Technology Systems Security Requirement (FedRAMP) For Unclassified Cloud Contract

Insert the clause at H- in all solicitations and contracts (including Task Orders) for information systems in the cloud computing environment.

FEDERAL INFORMATION TECHNOLOGY SYSTEMS SECURITY REQUIREMENT (FedRAMP) FOR UNCLASSIFIED CLOUD CONTRACT (SEP 2016).

1. The Contractor shall be responsible for the following privacy and security safeguards.

- a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records and databases.
- b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- c) The contractor shall also comply with any additional FedRAMP privacy requirements.
- d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government.
- e) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. *Exception – Disclosure to a Consumer Agency for purposes of C&A verification.* Contractor under this contract or otherwise provided by the Government. *Exception – Disclosure to a Consumer Agency for purposes of C&A verification.*
- f) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and
- Government specified tools.

g) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of contractor conducted scans shall be provided, in full, to the Government.

2. *Sensitive Information Storage:*

For Official Use Only (FOUO) information, data, and/or equipment will only be disclosed to authorize personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *Guidelines for Media Sanitization*.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed.

3. *Protection of Information:*

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

Government data loaded into or processed by the cloud services shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

4. *Security Classification:*

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level.

5. *Confidentiality and Nondisclosure:*

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the

conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-14.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

6. Disclosure of Information:

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

7. Security Requirements Section:

The minimum requirements for low, moderate and high impact level cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and Joint Authorization Board (JAB) will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

DOT will be able to leverage the provisional Authorization granted by FedRAMP, and agency issued FedRAMP authorizations, and any documentation prepared by the contractor to issue their own authority to operate in accordance with *DOT Security Authorization & Continuous Monitoring Performance Guide*.

The contractor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at <http://FedRAMP.gov>.

8. *FedRAMP Security Compliance Requirements:*

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low, moderate, and high impact level systems (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

9. *Required FedRAMP Policies and Regulations:*

OMB Memo Security Authorization of Information Systems in Cloud Computing Environments

10. *Assessment and Authorization:*

The Agency may choose to cancel the (Contract/award) and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

11. *Assessment of the System:*

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the documentation using FedRAMP requirements and templates, which are available at <http://FedRAMP.gov>.
2. Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
3. The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device

scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

4. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require POA&Ms to be remediated before a provisional or agency authorization is issued.

5. The contractor is responsible for mitigating all security risks found during Authorization &Assessment and continuous monitoring activities. All vulnerabilities must be mitigated within 7 days for critical, 30 days for high, 60 days for medium, 90 days for lows and at the discretion of the Authorizing Official for informational vulnerabilities from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

12. *Authorization o/System:*

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

13. *Reporting and Continuous Monitoring:*

Maintenance of the FedRAMP Provisional or DOT-issued Authorizations will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables allow the FedRAMP JAB and/or DOT to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

14. *Audit, Inspection, and Access:*

The contractor shall respond to government requests for documentation and/or access to the contractor facilities for any lawful government purpose to include oversight, audit, and inspection within a reasonable period of notification from the government not less than two (2) business days unless otherwise negotiated as specific terms within the governing contract. The contractor shall provide access and documentation without requirement for separate or additional non-disclosure. The government commits to the contractor that information provided by the contractor shall be retained no longer than required by law or applicable Department/ Agency policy, shall be appropriately protected while within the government's possession, and shall be

destroyed in accordance with Federal requirements for the destruction of sensitive information and media when no longer required.

Additional Stipulations:

1. The FedRAMP deliverables shall be labeled "FOR OFFICIAL USE ONLY" (FOUO) or other label as determined by the Government per document sensitivity. External transmission/dissemination of deliverables labeled FOUO or similar marking or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."
2. As prescribed in the Federal Acquisition Regulation (FAR) Part 24.104, if the system involves the design, development, or operation of a system of records on individuals, the contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act."
3. The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.