

For Official Use, Only
Version 2

Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook

OFFICE OF INFORMATION TECHNOLOGY SERVICES

December 2017



U.S. Department
of Transportation

**Federal Highway
Administration**

This Page Intentionally Left Blank

Authority

This United States Department of Transportation (DOT) *Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook* has been developed by FHWA to further its statutory responsibilities under DOT and FHWA policies. In accordance with the United States DOT, *Departmental Cybersecurity Compendium*, dated June 2015, Policy Identification (DOT-PM-1), FHWA is responsible for ensuring compliance with DOT cybersecurity policies and procedures and, as such, this Handbook ensures that compliance. Nothing in this Handbook should be taken to contradict the standards and guidelines made mandatory and binding on DOT Components by DOT Order 1351.37, as amended, *Departmental Cybersecurity Policy*, Chief Information Officer Policy (CIOP) Chapter 37 under statutory authority. Nor should this Handbook be interpreted as altering or superseding the existing authorities of DOT Order 1351.37. This Handbook will be reviewed on an annual basis and updated as necessary based on that review.

This Handbook sets forth the FHWA cybersecurity program:

- Which adopts/inherits DOT's cybersecurity policies and procedures described in DOT Order 1351.37 and its associated Compendium;
- Ensures consistency throughout FHWA in applying the policies, processes, procedures, and standards of the DOT Cybersecurity Program; and
- Identifies FHWA specific cybersecurity policies, processes, procedures, and standards for those cybersecurity areas where DOT has requested definition at the DOT Component level or where FHWA as a DOT Component is allowed to tailor the DOT Cybersecurity Program to provide adequate protection for FHWA information systems and the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction.

Furthermore, in accordance with DOT Order 1351.37, as the FHWA Chief Information Officer (CIO), I designate myself as the Authorizing Official (AO) for all information and information systems that support the operations and assets of FHWA, including those provided or managed by another agency, contractor or other source on behalf of FHWA.

As the FHWA CIO, I am committed to the delivery of mission-focused information technology solutions and services with the appropriate cybersecurity assurances as detailed in this Handbook.



Sarah J. Shores
Associate Administrator for Administration



Date

This Page Intentionally Left Blank

Table of Contents

INTRODUCTION.....	1
1.1 PURPOSE.....	2
1.2 APPLICABILITY	2
1.3 REFERENCES	2
1.4 ORGANIZATION OF THIS HANDBOOK.....	2
1.5 ROLES AND RESPONSIBILITIES.....	3
1.6 WAIVERS.....	4
CYBERSECURITY FUNCTIONAL PROGRAM AREAS	6
2.1 PROGRAM MANAGEMENT (PM)	7
2.2 ACCESS CONTROL (AC)	7
2.3 SECURITY AWARENESS AND TRAINING (AT)	8
2.4 AUDIT AND ACCOUNTABILITY (AU)	9
2.5 SECURITY ASSESSMENT AND AUTHORIZATION (CA)	9
2.6 CONFIGURATION MANAGEMENT (CM).....	10
2.7 CONTINGENCY PLANNING (CP)	10
2.8 IDENTIFICATION AND AUTHENTICATION (IA).....	11
2.9 INCIDENT RESPONSE (IR).....	11
2.10 MAINTENANCE (MA).....	11
2.11 MEDIA PROTECTION (MP)	11
2.12 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE).....	13
2.13 PLANNING (PL)	13
2.14 PERSONNEL SECURITY (PS)	13
2.15 RISK ASSESSMENT (RA)	14
2.16 SYSTEM AND SERVICES ACQUISITION (SA)	14
2.17 SYSTEM AND COMMUNICATIONS PROTECTION (SC)	14
2.18 SYSTEM AND INFORMATION INTEGRITY (SI).....	14
2.19 OTHER DOT POLICY FAMILIES NOT PREVIOUSLY LISTED	15

APPENDICES

APPENDIX A	FHWA REQUIREMENTS FOR THE DOT CYBERSECURITY COMPENDIUM WORKBOOK
APPENDIX B.....	ACRONYMS
APPENDIX C.....	ISSM DESIGNATION LETTER
APPENDIX D	FHWA IT SECURITY INCIDENT REPORTING PROCEDURES
APPENDIX E	FHWA INFORMATION SECURITY IN THE SYSTEM DEVELOPMENT LIFE CYCLE
APPENDIX F.....	FHWA MEDIA SANITIZATION REQUEST PROCEDURES
APPENDIX G	FHWA BUSINESS IMPACT ANALYSIS METHODOLOGY AND QUESTIONNAIRE

Record of Change

The following changes have been incorporated into FHWA CSP Handbook.

[illegible]

CHAPTER ONE

INTRODUCTION

THE NEED TO PROTECT INFORMATION AND INFORMATION SYSTEMS

The Federal Highway Administration (FHWA) Cybersecurity Program (CSP) is an FHWA-wide program which provides cybersecurity protections for the information and information systems that support the operations and assets of FHWA, including those provided or managed by another agency, contractor or other source on FHWA's behalf. The FHWA CSP Program encompasses all FHWA information, data, and resources collected, stored, processed, disseminated, or transmitted using FHWA information technology (IT) systems, to include the physical facilities in which the information, data and resources are housed.

The FHWA CSP adopts/inherits all components of the Department of Transportation (DOT) Cybersecurity program and its supporting policy and procedures as indicated within this document. In addition, Appendix A of this document contains those controls from the DOT Cybersecurity Compendium Workbook for which one or more parameters have been identified by DOT as "Component Defined" or for which specification is required by the Component.

In addition, FHWA, as a DOT Component, has implemented or will implement, as required, FHWA specific cybersecurity policies, guidance, and procedures to supplement and/or compliment the DOT Cybersecurity Program as defined in DOT Order 1351.37 Departmental Cybersecurity Policy and its associated Departmental Cybersecurity Compendium.

The FHWA CSP Handbook is comprised of policies, procedures, and guidance for ensuring the security of FHWA information and information systems. It encompasses cybersecurity management, planning, implementation, and performance evaluation. The FHWA CSP Handbook covers all IT resources, including, but not limited to, computers, computer room facilities, networks, telecommunications systems, applications, data, and information. Cybersecurity is a concept and operational feature that must be reflected in FHWA business process improvement efforts, as well as IT capital planning and investment selection criteria, and documentation of current and target enterprise architectures. In an overall sense, the objective of the FHWA Cybersecurity Program Handbook is to define, develop, implement, administer, maintain and update, as needed, those security controls necessary and sufficient to provide an acceptable level of security risk, at an acceptable level of cost, for each FHWA information system.

Benefits of the FHWA CSP Handbook are:

- Protection of FHWA sensitive information in accordance with Office of Management and Budget (OMB) Circular A-130 (including all appendices), *Management of Federal Information Resources*, revised July 27, 2016.
- Compliance with the DOT Cybersecurity Program and assurance that all information, regardless of sensitivity, is treated in an appropriate and secure manner.
- Management of risk to ensure that the level of risk is kept at an acceptable level and adequate risk mitigation is employed.
- Assurance that safeguards for the protection of the integrity, availability, and confidentiality of FHWA information and information systems are integrated into and support the missions of FHWA.

- Assurance that security requirements and capabilities are represented at all levels of the current and target FHWA enterprise architectures. These levels are business, data, application, and technical, and in combination, represent an integrated view of the business/technology operating environment of the enterprise.
- Integration of security throughout the life cycle of a system from project conception through its replacement or disposal.
- Assurance that FHWA critical IT operations and infrastructures remain operational by identifying and correcting IT vulnerabilities before they impact the operational environment.

The FHWA CSP Handbook exists as a living document, subject to additions, deletions, and/or content modifications based on changing requirements, technology, and threats, as deemed necessary.

1.1 PURPOSE

The FHWA CSP Handbook:

- Ensures FHWA's compliance with the Departmental Cybersecurity Policy, DOT Order 1351.37, and its associated Departmental Cybersecurity Compendium.
- Ensures consistency throughout FHWA in applying the policies, processes, procedures and standards of the DOT Cybersecurity Program.
- Identifies FHWA specific cybersecurity policies, processes, procedures and standards for those cybersecurity areas where DOT has requested definition at the DOT Component level or where FHWA as a DOT Component is allowed to tailor the DOT Cybersecurity program to provide adequate protection for FHWA information systems and the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction.

1.2 APPLICABILITY

The FHWA CSP Handbook applies to all FHWA employees, contractors and subcontractors and other users of FHWA information and information systems. It also applies to information and information systems that support FHWA's operations and assets, including those provided or managed by another Federal agency, a contractor, or another source.

1.3 REFERENCES

- *DOT Order 1351.37, Departmental Cybersecurity Policy*, as amended
- *Departmental Cybersecurity Compendium*, as amended
- *Security Authorization & Continuous Monitoring Performance Guide*, as amended
- *Automated Enterprise Continuous Monitoring (AECM) System Guide*, February 20, 2013
- *Security Weakness Management Guide*, September 2013
- *FISMA Inventory Guide*, September 2013
- *DOT Cybersecurity Incident Response Plan (IRP)*, as amended

1.4 ORGANIZATION OF THIS HANDBOOK

This document is organized into sections which provide information on the FHWA Cybersecurity Program as follows:

Section Number	Description
1.0	INTRODUCTION – Provides an overview of the FHWA Cybersecurity Program and its relation to the DOT Cybersecurity Program.
1.1	PURPOSE – lists the overall purpose of the FHWA Cybersecurity Program
1.2	APPLICABILITY – describes the individuals, FHWA information, and information systems the program applies to
1.3	REFERENCES – lists the documents that are commonly cited within this handbook
1.4	ORGANIZATION OF THIS HANDBOOK – describes the sections of this document.
1.5	ROLES AND RESPONSIBILITIES – Describes specific roles and responsibilities for the FHWA Cybersecurity Program
1.6	WAIVERS – describes the waiver process
Chapter 2	FUNCTIONAL PROGRAM AREAS – Describes the FHWA Cybersecurity program areas and their alignment with the DOT Cybersecurity Compendium Workbook

1.5 ROLES AND RESPONSIBILITIES

The DOT Order 1351.37 identifies the cybersecurity responsibilities for various roles at all levels in the Department including DOT Component Specific roles.

The following are further clarifications pertaining to FHWA for the roles and responsibilities listed within the DOT Order 1351.37¹.

Component Chief Information Officer (CIO):

The FHWA Associate Administrator for Administration has been appointed as the FHWA CIO.

Deputy CIO:

The FHWA CIO has appointed the Director, Office of Information Technology Services to serve as Deputy CIO. Responsibilities are to act in the absence of the FHWA CIO and to perform specific functions of the FHWA CIO as identified in writing.

Component Information System Security Manager (ISSM):

FHWA ISSM primary responsibilities are the ISSM cybersecurity responsibilities as defined in DOT Order 1351.37. The ISSM appointment letter is included in Appendix C of this document.

Component Chief Privacy Officer

The FHWA Associate Administrator for Administration is the FHWA Chief Privacy Officer. However, a member of the IT Policy Team within the Office of Information Technology Services has been designated as the FHWA Privacy Liaison and serves as the FHWA Point of Contact for operational privacy functions.

Component Risk Executive

As defined in section 37.5.13 of DOT Order 1351.37, the Risk Executive function must be assigned to an individual or group. If an organization has more than one Authorizing Official (AO), those AOs would come together and perform the risk executive function. FHWA has one Authorizing Official (AO) by default this AO is the FHWA Risk Executive. The FHWA Associate Administrator for Administration is the FHWA Risk Executive.

¹ Specific cybersecurity responsibilities for these roles can be found in DOT Order 1351.37.

Authorizing Official (AO)

The FHWA CIO serves as the FHWA AO.

Information Systems Security Officer (ISSO)

An ISSO must be appointed for each information system and is responsible for ensuring the security of the information system and that the information system complies with information security requirements throughout the System Development Life Cycle (SDLC) (from design through disposal). In FHWA, the ISSO appointment is documented in the Security Plan for the information system. An individual may serve as the ISSO for more than one system and can be either a Federal Government employee or an FHWA contractor. However, the appointment of a contractor as an ISSO for an FHWA information system must be approved by the FHWA AO.

System Owner (SO)

A SO must be appointed for each information system and is responsible for procuring, developing, integrating, modifying, or operating and maintaining the FHWA information system and relying on the assistance and advice of the ISSM, information system operators, and other IT staff in the implementation of security responsibilities. A SO must be a Federal Government employee.

Information Owner (IO)

As defined in section 37.5.27 of DOT Order 1351.37 IOs are Federal Government employees/officials with statutory or operational authority for specific information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. However, a single information system may utilize information from multiple Information Owners. In FHWA, unless it is specified in the Information System's Security Plan, the System Owner is the Information Owner for all information created, modified, processed, etc. by the information system.

External Provider and Third Party

In addition to the roles previously identified in this section, the DOT Cybersecurity Compendium refers to "external provider" and "third party". The following definitions for these roles are:

- **External Provider:** A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (Example: A contractor that does not have a direct contract with FHWA; however, provides services for FHWA.)
- **Third Party:** Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. (Example: A contractor hosting facility that has a direct contract with FHWA.)

1.6 WAIVERS

DOT Cybersecurity policy as defined in DOT Order 1351.37 and its associated Compendium are mandatory within DOT. Therefore, should the need for a waiver to DOT cybersecurity policy present itself within FHWA, the FHWA waiver request must comply with and adhere to Section 37.9 of DOT Order 1351.37. Before proceeding with a waiver request the FHWA ISSM must be contacted to ascertain if a waiver is possible and to coordinate the request with DOT.

In the event that a waiver is required for any specific FHWA cybersecurity policies, procedures, standards or processes that are unique to FHWA and not identified in DOT Order 1351.37 and its Compendium, the FHWA ISSM must be contacted to ascertain if a waiver is possible.

CHAPTER TWO

CYBERSECURITY FUNCTIONAL PROGRAM AREAS

SECURITY CONTROL FAMILIES, BASELINES, AND ASSURANCE

The DOT Cybersecurity Policy, DOT Order 1351.37, as amended, is supplemented by the Departmental Cybersecurity Compendium which contains information technology and cybersecurity policy, guidance and standards. Appendix F of the Compendium contains the Compendium Security Control Workbook

The Security Control Workbook specifies supplemental DOT Cybersecurity policy. The policy is organized into "families" with corresponding abbreviations, for example Access Control (AC). The majority of the families in the Workbook directly relate to the NIST SP 800-53 Revision 4 security control families. However, the Workbook does contain some additional DOT-specific policy families and various appendices that are not included among the NIST 800-53 Revision 4 security control families.

FHWA's compliance with specific policies identified in several of the policy families represented in the Workbook depend upon FHWA receiving certain IT Services provided by the DOT Common Operating Environment (COE). These services are electronic mail (e-mail) and network services including remote access mechanisms to the DOT network. Therefore, FHWA organizations are prohibited from installing and maintaining their own electronic mail systems, networks or remote access mechanisms. Furthermore, FHWA organizations must obtain approval from the COE prior to acquiring or implementing wireless access points. Additionally, there is a government-wide initiative to reduce the number of government data centers. Therefore, no FHWA organization may set up a new data center or have a contractor or other entity set up one on their behalf.

The FHWA CSP has numerous cybersecurity functional program areas that align with the various policy families identified in the DOT Workbook. The remainder of this section describes the FHWA CSP areas considering their relation to the DOT Workbook policy families. It is anticipated that over time DOT will add or delete policy families from the Security Control Workbook. Every effort will be made to keep the FHWA Cybersecurity functional program areas aligned with these changes but in the event, the Workbook includes a policy family that the FHWA CSP Handbook does not have documented, then that policy family will be included by default in the FHWA CSP Handbook exactly as stated in the Workbook. In the event that a policy family is removed from the Workbook and the FHWA CSP Handbook has not reflected the removal in the CSP documentation, then the FHWA CSP functional area relating to that policy family will be considered to no longer be an area included in the FHWA CSP.

CAUTIONARY NOTE

IMPLEMENTING SECURITY CONTROLS BASED ON THIS HANDBOOK

The DOT and NIST security controls cited are not always the complete control: only what needs clarification. All DOT security control objectives must be documented and tested accordingly.

2.1 PROGRAM MANAGEMENT (PM)

The FHWA Program Management functional area adopts/inherits all DOT policies and procedures pertaining to program management as defined in DOT Order 1351.37 and its Compendium with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
PM-3	DOT-PM-3	FHWA uses NIST SP 800-65 guidance to incorporate Security priorities in the Capital Planning process. In accordance with NIST SP 800-53 during the Capital Planning Process FHWA does the following: <ul style="list-style-type: none"> Includes an assessment of information security requirements for the information system in the investment planning process; Determines, documents, and allocates the resources required to protect the information system; and Reports security costs in the Exhibit 300 security investment which includes the security costs for all investments. Additional security costs are also reported in the Budget Data Request (BDR). All Capital Planning and Investment Control (CPIC) reporting is in accordance with OMB Circular A-11 and annually updated CPIC reporting guidance.
PM-4	DOT-PM-4	System Owners must ensure that corrective actions listed in the plan of action and milestones (POA&Ms) for their system are remediated by the date established when the POA&Ms were created to prevent an overdue status condition for a POA&M. If not remediated by that date they must notify the FHWA ISSM of a new target completion date. However, the POA&M will still be considered overdue until remediated and closed.
PM-5	DOT-PM-5.a	FHWA must request updates to the DOT Federal Information Security Management Act (FISMA) Inventory for FHWA information systems as changes occur.
PM-7	DOT-PM-7.b	Cybersecurity must be fully integrated into FHWA's Enterprise Architecture (EA) and consistent with the FHWA CSP and DOT's EA program.
PM-8	DOT-PM-8.e	The FHWA ISSM annually notifies the DOT CISO if any FHWA physical or Cyber assets are potential Critical Infrastructure Protection candidates.

2.2 ACCESS CONTROL (AC)

The FHWA CSP Access Control Functional area adopts/inherits all applicable DOT policies and procedures pertaining to access control as defined in DOT Order 1351.37 and its Compendium with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
AC-2	DOT-AC-2.i	FHWA may revoke the access of a user to DOT/FHWA information systems for the following reasons: <ul style="list-style-type: none"> Unauthorized use of DOT/FHWA information system

		<ul style="list-style-type: none"> • Conduct that interferes with the normal and proper operation of DOT/FHWA information systems; • Activities that adversely affect the ability of others to use DOT/FHWA information systems; • Activities that are harmful or offensive to others; • Violation of valid rules of behavior (e.g., general or system specific) that was acknowledged by a user; • In-the-event the System Owner and ISSM determines that illegal or other unscrupulous activities have been enacted on a DOT/FHWA information system. <p>To revoke the access of a user for any of the above listed reasons, the FHWA ISSM must be contacted by telephone and email. The contact must include the reason for the revocation. If the ISSM agrees, the ISSM will take the necessary action to revoke the access and will notify the requestor to provide appropriate documentation of the revocation request including the reason for the revocation. The ISSM will provide the requestor with a written response to the request detailing the actions the ISSM took. Additionally, such behavior could result in oral or written warning, reassignment to other duties, criminal or civil prosecution, or suspension from duty and/or termination of employment for federal employees, or removal from a contract for contractor personnel. Consequences of failure to comply will be commensurate with the individual's level of responsibility and the nature of the violation.</p>
AC-5	DOT AC-5	Separation of duties for each FHWA IT system is documented within the System Technical Architecture Document (formerly called the System Overview) or the Security Plan.

2.3 SECURITY AWARENESS AND TRAINING (AT)

FHWA provides security awareness training and specialized security training consistent with DOT policy and procedures. For security awareness training DOT provides training that FHWA employees and contractors must take. Specialized security training for FHWA employees and contractors is determined by the FHWA ISSM and is consistent with DOT policy.

All FHWA employees and contractors that have access to FHWA and/or DOT information systems are required to receive security awareness training initially upon joining FHWA and annually thereafter. New Contractors must provide evidence of completing the security awareness training before they are given access to FHWA/DOT information systems. New FHWA employees are to take the training prior to their entry on duty date.

FHWA contractor employees that do not have a DOT/FHWA network ID, access to DOT/FHWA facilities and access to DOT/FHWA IT systems/information do not have to complete annual IT security awareness training. FHWA contractors that only have access to DOT/FHWA facilities do not have to complete annual IT security awareness training but they should be provided with physical security training by the facility manager for those facilities for which the contractor has access.

The FHWA CSP security awareness and training functional area adopts/inherits all applicable DOT policies and procedures pertaining to security awareness and training as defined in DOT Order 1351.37 and its Compendium with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification

AT-2	DOT-AT-2.d	For FHWA the personnel and payroll system that DOT uses are the authoritative source of FHWA active employees. The authoritative source for active FHWA contractors is the file maintained by the Office of Acquisition and Grants Management (HCFA) from information provided by FHWA CORs. All FHWA employees and contractors are considered to be users of FHWA/DOT information systems and therefore, are required to take Security Awareness Training unless a documented exception exists. Since the Active Directory for DOT represents the largest community of DOT information users, FHWA validates those FHWA users listed in the DOT Active Directory against our authoritative sources of FHWA employees and contractors and reconciles any differences.
AT-4	DOT-AT-4.b	System Owners of FHWA systems must document in their system documentation (i.e., security plan or Technical Architecture Document (formerly called System Overview)) how user accounts are distinguished from system accounts.

2.4 AUDIT AND ACCOUNTABILITY (AU)

The FHWA CSP audit and accountability functional area adopts/inherits all DOT policies and procedures pertaining to audit and accountability as defined in DOT Order 1351.37 and its Compendium with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
AU-4	DOT-AU-4.a	All FHWA general support systems and IT applications must maintain the ability to log five contiguous days online of security events at the highest level of details without exceeding 85% of the available storage allocated for online log storage. Additionally, a minimum of one year's worth of security event logs must be retained though they can be retained in an offline state. This is in addition to any established record retention schedules.
AU-6	DOT-AU-6	FHWA requires that system audit records from FHWA general support systems must be reviewed daily and audit records for FHWA major applications must be reviewed at least monthly.

Separation of Duties

PLEASE NOTE: To ensure separation of duties in reviewing audit logs, individuals being audited cannot be the sole individuals reviewing the audit logs.

2.5 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

The FHWA CSP security assessment and authorization control functional area adopts/inherits all applicable DOT policies and procedures pertaining to security assessment and authorization as defined in DOT Order 1351.37 and its Compendium to include the *Security Authorization & Continuous Monitoring Performance Guide* version 4.0, dated February 2016, and the *Security Weakness Management Guide* version 2.0, dated March 2017, with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
---------------------	---------------	--------------------

CA-1	DOT-CA-1. g	If the information system is categorized as a cloud computing resource, DOT Components must follow guidance from the DOT issued via Cybersecurity Action Memo. If this guidance is not available, Components must follow current guidance from OMB and the FedRAMP program office. Only cloud service providers (CSPs) with a FedRAMP Agency issued ATO or a FedRAMP Joint Authorization Board (JAB) Provisional ATO can be used for FHWA.
CA-3	DOT-CA-3.c	Interconnections of an FHWA system that extend to systems outside of FHWA must be authorized by the Authorizing Official prior to allowing the interconnection.
CA-7(1)	DOT-CA-7(1)	All FHWA systems are required to use the FHWA Continuous Monitoring (CM) process to monitor the security controls on an ongoing basis unless an official waiver is requested and approved by Authorizing Official.

Furthermore, to ensure compliance with DOT's security assessment and authorization process, documented within Appendix G of this handbook are the FHWA Security Assessment and Authorization Procedures.

2.6 CONFIGURATION MANAGEMENT (CM)

The FHWA CSP configuration management functional area adopts/inherits all applicable DOT policies and procedures pertaining to configuration management as defined in DOT Order 1351.37 and its Compendium which includes the *Automated Enterprise Continuous Monitoring (AECM) System Guide*, dated February 20, 2013 with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
CM-3	DOT-CM-3	All FHWA systems including systems with a sensitivity level of low must follow and participate in the FHWA Change Management Process.
CM-6	DOT-CM-6	While DOT OCIO maintains a list of approved configuration baselines and deviations, the FHWA ISSM decides which baselines can be used within FHWA.
CM-9	DOT-CM-9	NIST defines configuration items as the information system items (hardware, software, firmware, and documentation) to be configuration managed. FHWA subscribes to this definition.

Change Management

PLEASE NOTE: For all FHWA information systems, changes must follow a documented process that includes an FHWA ISSM/ISSO signature to ensure that the impact of the change on the security posture of the system has been evaluated.

2.7 CONTINGENCY PLANNING (CP)

The FHWA CSP contingency planning control functional area adopts/inherits all applicable DOT policies and procedures pertaining to contingency planning. Additionally, the system owner should review the contingency plan for the information system as a part of each significant change to the information system.

FHWA's Office of Information Technology Services (OITS) provides for alternate site processing for mission critical applications that OITS supports in the event that primary site processing is expected to be unavailable for a prolonged period of time as determined by FHWA senior management. Mission critical applications are replicated to the alternate processing site and can be available within 24 hours at the alternate site if the decision is made to implement alternate site processing.

OITS also provides alternate site processing for business essential applications that OITS supports. Business essential applications will be made available at the DR site as soon as practical after the mission critical applications have been made available at the alternate site.

Ultimately, FHWA system owners are responsible for ensuring that their alternate site processing needs are adequately addressed.

2.8 IDENTIFICATION AND AUTHENTICATION (IA)

The FHWA CSP identification and authentication control functional area adopts/inherits all applicable DOT policies and procedures pertaining to identification and authentication.

FHWA employees and contractors shall not share, modify, or destroy authenticators such as Personal Identity Verification (PIV) cards, tokens, smart cards, or key cards assigned to them for unique identification and authentication on information systems and treat said authenticators as FHWA/DOT property to be protected and secured when not in use.

All FHWA applications and systems as well as those developed for FHWA must require use of the PIV card for identification and authentication. This includes Commercial Off the Shelf (COTS) products.

2.9 INCIDENT RESPONSE (IR)

The FHWA CSP incident response control functional area adopts/inherits all applicable DOT policies and procedures pertaining to incident response. However, by subscribing to the DOT Security Operations Center (DOT SOC) for incident response, FHWA complies with DOT incident response policies and procedures. While the DOT SOC provides incident response for DOT including FHWA, FHWA does provide contractor support resources that offer advice and assistance for the handling and reporting of security incidents.

The FHWA ISSM is the point of contact for coordinating incident response between the DOT SOC and FHWA.

Appendix D contains the FHWA— incident reporting procedures that FHWA employees and contractors must comply with.

2.10 MAINTENANCE (MA)

The FHWA CSP maintenance control functional area adopts/inherits all applicable DOT policies and procedures pertaining to maintenance control.

2.11 MEDIA PROTECTION (MP)

For purposes of understanding DOT's media protection policies as described in DOT 1351.37 and its associated Compendium, FHWA defines digital media to include but is not limited to flash drives, thumb drives, USB devices, external and internal computer hard drives magnetic tapes,

compact discs, diskettes, digital video disks, tablet, laptop and notebook computers, smartphones, network attached storage devices, and other electronic devices which have information storage capability. FHWA further defines non-digital media to include but not limited to printed documents, paper files, books, photographs, maps, diagrams, forms, drawings and other printed or written materials.

Portable digital media that stores FHWA/DOT information must employ encryption that is NIST FIPS 140-2 validated. The FHWA ISSM provides assistance to FHWA employees and contractors regarding encryption.

When digital media that previously stored FHWA information is no longer needed, it must be sanitized before it is discarded or reused. Record retention schedules must be satisfied before sanitization can occur. Sanitization must be accomplished by completely wiping the information from the device. Simply deleting the information is not sufficient. There are both hardware and software methods of wiping information off the digital media that can be used. The hardware method involves using a device called a degausser. The digital media is placed in contact with the degausser and any information on the digital media is destroyed and cannot be recovered. For many forms of digital media such as hard drives and some tape backup devices, degaussing renders the media completely unusable and damages the storage system. Degaussing cannot be used on a computer hard drive if the computer is to be used again, for example reassigned to another office or donated to a school system. In those cases, software capable of wiping information from a hard drive must be used.

The FHWA ISSM has setup a process whereby FHWA field and other remote offices can send their digital media to HQ to be destroyed. The media is sent to the FHWA ISSM. Appendix D includes the procedure to be followed for sending media to HQ for destruction and includes the necessary form and instructions. Field/remote offices that have large quantities of digital media requiring degaussing, where sending the media to HQ would not be cost effective, should contact the FHWA ISSM to identify an alternative for performing the destruction locally. Procedures for excessing computer equipment at HQ include provisions for sanitizing digital media. However, any HQ offices that need to sanitize external hard drives or other storage media not normally included in computer excessing procedures need to contact the FHWA ISSM to arrange to have the media sanitized. FHWA offices needing to use a software method for wiping information from a hard drive or other digital media should contact the FHWA ISSM to identify an approved software product that the office can acquire.

Non-digital media that contains sensitive information when no longer needed must be destroyed in such a way that the information cannot be retrieved or accessed in any manner. Record retention schedules must be satisfied before destruction occurs. Shredding or other destruction methods such as incineration must be employed. Most FHWA offices have shredders placed throughout the office areas and for large quantities of non-digital media have arranged with an external company to take the non-digital media offsite for destruction. FHWA staff requiring assistance or having questions about destruction of non-digital media with sensitive information should contact the FHWA ISSM.

The FHWA CSP media protection control functional area adopts/inherits all applicable DOT policies and procedures pertaining to media protection with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
---------------------	---------------	--------------------

MP-2	DOT-MP-2	FHWA information owners must restrict access to FHWA information stored on digital and non-digital media to only those individuals with a need to know. In order to restrict access, logical and/or physical measures must be employed.
MP-2	DOT-MP-2.d	All FHWA employees and contractors cannot process or store FHWA information in digital form on non-DOT/non-FHWA issued media unless approved in writing by the FHWA ISSM. This includes but is not limited to the digital media types described at the beginning of section 2.11 of this handbook. Please note that non-DOT issued media includes the hard-drive of a personally owned desktop or laptop computer, personally owned tablet computers including iPads, personally owned cell phones that are not included in DOT's mobile device management program (MDM) which includes the installation of the Good Software on the device. Furthermore, when using flash/thumb drives or external hard drives only self-encrypting drives can be used. FHWA StaffNet contains information on makes and models of approved self-encrypting drives
MP-5	DOT-MP-5	The use of DOT provided laptops, tablet computers, cell phones, blackberries while on personnel foreign travel (i.e., travel outside the United States and its territories) is prohibited. The use of DOT provided laptops, tablet computers, cell phones, blackberries while on business foreign travel must comply with all DOT policies on international travel, including the use of loaner equipment and comply with the DOT Rules of Behavior regarding Foreign travel.

2.12 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

The FHWA CSP physical and environmental protection functional area adopts/inherits all applicable DOT policies and procedures pertaining to physical and environmental protection with the following clarification.

NIST Control Number	DOT Policy Id	FHWA Clarification
PE-18	DOT-PE-18.a	FHWA organizations may not construct or create new data centers. Furthermore, FHWA IT information systems must be in a hosting facility or data center approved by the DOT CIO. The process to get a hosting facility or data center approved by the DOT CIO requires the approval of the FHWA ISSM who will obtain the DOT CIO approval.

2.13 PLANNING (PL)

The FHWA CSP planning security functional area adopts/inherits all applicable DOT policies and procedures pertaining to planning.

2.14 PERSONNEL SECURITY (PS)

The FHWA CSP personnel security functional area adopts/inherits all applicable DOT policies and procedures pertaining to personnel security with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
PS-8	DOT-PS-8.a	Refer to DOT control DOT-AC-2.i in section 2.2 of this handbook for a list of reasons FHWA may revoke the access of a user to DOT/FHWA information systems.

2.15 RISK ASSESSMENT (RA)

The FHWA CSP risk assessment functional area adopts/inherits all applicable DOT policies and procedures pertaining to risk assessment which includes the *Automated Enterprise Continuous Monitoring (AECM) System Guide*, dated February 20, 2013. with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
RA-5	DOT-RA-5	As of October 2017, FHWA's general support systems are scanned daily by DOT OCIO.

2.16 SYSTEM AND SERVICES ACQUISITION (SA)

The FHWA CSP system and services acquisition functional area adopts/inherits all applicable DOT policies and procedures pertaining to system and services acquisition with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
SA-3	DOT-SA-3	Appendix E of this document describes the FHWA System Development Life Cycle (SDLC) and outlines the security activities that take place at each of the five phases of the SDLC.
SA-4	DOT-SA-4.d	Production data whether sensitive or non-sensitive cannot be used on non-production systems without the approval of the FHWA ISSM.

2.17 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

In keeping with DOT's IT shared service initiative, FHWA depends upon the DOT COE for network services. That includes the adoption of the intrusion detection system (IDS) /intrusion protection system (IPS) policies and procedures as promulgated by the DOT SOC and the COE. The FHWA CSP system and communications protection functional area adopts/inherits all applicable DOT policies and procedures pertaining to system and communications protection with the following clarifications.

NIST Control Number	DOT Policy Id	FHWA Clarification
SC-18	DOT-SC-18	FHWA controls the use of Mobile code and mobile technologies by requiring that System Owners obtain written approval from the FHWA ISSM for the use of mobile code and mobile code technologies before they are deployed in FHWA information systems. Furthermore, the use of mobile code and mobile code technologies for an information system must be explicitly identified and completely documented in the security plan or technical architecture document for the information system.
SC-19	DOT-SC-19	FHWA non-HQ organizations implementing Voice Over Internet Protocol (VOIP) phone systems must obtain approval from FHWA's Office of Information Technology Services (OITS) prior to purchasing a system. Once the system has been acquired it must be configured in accordance with FHWA and DOT's COE requirements.

2.18 SYSTEM AND INFORMATION INTEGRITY (SI)

Commercial Off-The-Shelf (COTS) software must be properly updated to reflect improvements, changes, and fixes supplied by the COTS vendor. It is DOT policy that only current and up-to-

date COTS software products that are fully supported by the vendor are to be used by DOT/FHWA IT systems. Out-of-date and/or unsupportable software poses an unacceptable risk to DOT/FHWA IT systems in that the products cannot be patched if security vulnerabilities are discovered in the product. Furthermore, if problems with the product occur, the vendor often will not provide support for out-of-date software. Therefore, all FHWA IT systems utilizing COTS software must adhere to standard FHWA upgrade and patch implementation frequencies to ensure safe and timely installation and management of vendor-provided updates and patches/fixes to COTS software as follows:

SOFTWARE UPGRADES:

COTS major version upgrades must be completed within four months after the second newer major version's General Availability date. COTS minor release upgrades must be completed within four months after the vendor release date.

PATCHES AND FIXES:

The schedule for applying patches and fixes is based on how the patch has been identified and the characteristics of the patch/fix as follows:

- A patch/fix has been identified, either through a Vulnerability Report or through a review of available patches, which has an associated Common Vulnerabilities and Exposure (CVE) number or a known security flaw. In this case, depending on the severity of the vulnerability or security flaw the patch/fix must be applied within the following timeframes: 1 week for Critical/High, 2 weeks for Medium, 3 weeks for Low, and 4 weeks for Informational.
- The patch/fix has been identified, either through a Vulnerability Report or through a review of available patches, which does not have a CVE or a known security flaw associated with it. In this case, the patch/fix should be applied within one month of identification.

The FHWA CSP system and information integrity functional area adopts/inherits all applicable DOT policies and procedures pertaining to system and information integrity.

2.19 OTHER DOT POLICY FAMILIES NOT PREVIOUSLY LISTED

The FHWA CSP adopts/inherits all applicable DOT policies and procedures pertaining to these DOT control families and Appendices as identified in the Compendium. These include the DOT Cybersecurity Compendium additional DOT-specific policy families and various appendices that are not included amongst the NIST 800-53 Revision 4 Control families. Additionally, FHWA adopts/inherits all supplemental policies, guidance, procedures, standards and processes as promulgated by the DOT Chief Information Officer to implement mandatory cybersecurity requirements, which include but are not limited to Cybersecurity Action Memos, Technical Bulletins, Guides, Memorandums.

APPENDIX - A FHWA REQUIREMENTS FOR THE DOT CYBERSECURITY COMPENDIUM WORKBOOK

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Note: This Appendix contains those controls from the DOT component requirement of the DOT Cybersecurity Compendium Workbook for which one or more parameters have been identified by DOT as “Component Defined”. As a DOT Component, FHWA has defined those parameters in the following table. Furthermore, a “**Yes**” in the FIPS 199 Impact Level NIST SP 800-53 baseline security controls row with the three fields of L (Low), M (Moderate) and H (High) indicate the applicability of the policy to the information system based on the information system's FIPS 199 security categorization. Lastly, this Appendix contains FHWA’s clarifications or specific emphasis areas, as indicated by blue highlight.

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-AC-2.i	<p>FHWA Clarification</p> <p>FHWA may revoke the access of a user to DOT/FHWA information systems for the following reasons:</p> <ul style="list-style-type: none"> Unauthorized use of DOT/FHWA information system Conduct that interferes with the normal and proper operation of DOT/FHWA information systems; Activities that adversely affect the ability of others to use DOT/FHWA information systems; Activities that are harmful or offensive to others; Violation of valid rules of behavior (e.g., general or system specific) that was acknowledged by a user; In-the-event the System Owner and ISSM determines that illegal or other unscrupulous activities have been enacted on a DOT/FHWA information system. <p>To revoke the access of a user for any of the above listed reasons, the FHWA ISSM must be contacted by telephone and email. The contact must include the reason for the revocation. If the ISSM agrees, the ISSM will take the necessary action to revoke the access and will notify the requestor to provide appropriate documentation of the revocation request including the reason for the revocation. The ISSM will provide the requestor with a written response to the request detailing the actions the ISSM took. Additionally, such behavior could result in oral or written warning, reassignment to other duties, criminal or civil prosecution, or suspension from duty and/or termination of employment for federal employees, or removal from a contract for contractor personnel. Consequences of failure to comply will be commensurate with the individual’s level of responsibility and the nature of the violation.</p>				
DOT-AC-2(2) Account Management /Removal Of Temporary / Emergency Accounts	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].		Yes	Yes	The information system automatically [removes] temporary and emergency accounts after [Assignment: 30 days].

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-AC-2 (3) Account Management	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].		Yes	Yes	FHWA information system automatically disables inactive accounts after [Assignment: 90 days for all users except public users; FHWA System Owners may determine the time frame for public users but it must be less than or equal to 365 days].
DOT-AC-2 (5)	The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities].			Yes	FHWA information system implements the dynamic privilege management capabilities: [Assignment: as defined by the FHWA ISSM, if any.]
DOT-AC-5	FHWA Clarification Separation of duties for each FHWA IT system is documented within the System Technical Architecture Document (formerly called the System Overview) or the Security Plan.				
DOT-AC-6 (1)	The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].		Yes	Yes	FHWA explicitly authorizes access to [Assignment: all security functions (deployed in hardware, software, and firmware) and security-relevant information]. Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-AC-7 Unsuccessful Login Attempts	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	Yes	Yes	Yes	FHWA information system: a. Enforces a limit of [Assignment: 5] consecutive invalid logon attempts by a user during a [Assignment: 15-minute period]; and b. Automatically [locks the account/node for an [Assignment: 15 minutes or until released by administrator]] when the maximum number of unsuccessful attempts is exceeded.
DOT-AC-11 (1)	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.		Yes	Yes	FHWA information system conceals, via the session lock, information previously visible on the display with a publicly viewable image; such as patterns used with screen savers, photographic images, or a blank screen in which none of the images convey sensitive information
DOT-AC-17(2) Remote Access / Protection Of Confidentiality / Integrity Using Encryption	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.		Yes	Yes	FHWA information system implements NIST-validated cryptographic mechanisms [in accordance with FIPS 140-2] to protect the confidentiality and integrity of remote access sessions.
DOT-AC-18(1) Wireless	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.		Yes	Yes	FHWA information system protects wireless access to the system using authentication for both users and devices as well as employing

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Access / Authentication and Encryption					encryption techniques to prevent unauthorized disclosure of information during data transmission.
DOT-AC-18(4) Wireless Access / Configuration by Users	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.			Yes	Designated network administrators with the authorized <i>approval</i> of the FHWA ISSM are the only individuals authorized to independently configure wireless networking capabilities.
DOT-AC-19 Access Control For Mobile Devices	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	Yes	Yes	Yes	FHWA: a. requires all mobile devices to adhere to the COE established usage restrictions, configuration requirements, connection requirements, and implementation guidance for COE-controlled mobile devices; and b. the FHWA ISSM authorizes the connection of mobile devices to FHWA information systems.
DOT-AC-20(2) Use Of External Information Systems / Portable Storage Devices	The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.		Yes	Yes	The FHWA restricts the use of FHWA-controlled portable storage devices by authorized individuals on external information systems.
DOT-AC-21 Information Sharing	The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for		Yes	Yes	FHWA via the FHWA ISSM: a. Facilitates information sharing by enabling authorized users to determine whether access

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	[Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.				authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: Sensitive but Unclassified information to include PII]; and b. Employs [Assignment: FHWA change control process] to assist users in making information sharing/collaboration decisions.
DOT-AC-22 Publicly Accessible Content	The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.	Yes	Yes	Yes	In conjunction with FHWA Public Affairs review processes and procedures for public posting of information. FHWA System Owners: a. Designate individuals authorized to post information onto a publicly accessible FHWA information system; b. [ensures designate individuals authorized to post information onto a publicly accessible FHWA information system, obtain training] to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					system for nonpublic information [Assignment: quarterly] and removes such information, if discovered.
DOT-AT-2.d	<p>FHWA Clarification For FHWA the personnel and payroll system that DOT uses are the authoritative source of FHWA active employees. The authoritative source for active FHWA contractors is the file maintained by the Office of Acquisition and Grants Management (HCFA) from information provided by FHWA CORs. All FHWA employees and contractors are considered to be users of FHWA/DOT information systems and therefore, are required to take Security Awareness Training unless a documented exception exists.</p> <p>Since the Active Directory for DOT represents the largest community of DOT information users, FHWA validates those FHWA users listed in the DOT Active Directory against our authoritative sources of FHWA employees and contractors and reconciles any differences.</p>				
DOT-AT-4.b	<p>FHWA Clarification System Owners of FHWA systems must document in their system documentation (i.e., security plan or Technical Architecture Document (formerly called System Overview)) how user accounts are distinguished from system accounts.</p>				
DOT AU-2(3) Audit Events / Reviews and Updates	The organization reviews and updates the audited events [Assignment: organization-defined frequency].		Yes	Yes	FHWA reviews and updates the audited events [Assignment: annually or whenever there is a change in the threat environment].
DOT-AU-3 Content of Audit Records	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.		Yes	Yes	FHWA information systems are responsible for including the following information in their audit event records: For Systems; successful and unsuccessful account logins, account management events, object access, policy change, privileged functions, process tracking, system events and for Applications; administrator activity, authentication checks, authorization checks, data

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					deletions, data access, data changes, and permission changes.
DOT-AU-3(1) Content of Audit Records / Additional Audit Information	The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].		Yes	Yes	<p>The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon].</p> <p>Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.</p>
DOT-AU-3(2) Content of Audit Records / Centralized Management of Planned Audit Record Content	The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].			Yes	The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: the operating system, security software, and databases]
DOT-AU-4 Audit	The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].	Yes	Yes	Yes	FHWA allocates audit record storage capacity in accordance with [Assignment: Defense Information

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Storage Capacity					Systems Agency (DISA) STIG or Center for Internet Security (CIS) Benchmarks].
DOT-AU-4.a	FHWA Clarification All FHWA general support systems and IT applications must maintain the ability to log five contiguous days online of security events at the highest level of details without exceeding 85% of the available storage allocated for online log storage. Additionally, a minimum of one year's worth of security event logs must be retained though they can be retained in an offline state. This is in addition to any established record retention schedules				
DOT-AU-5(1) Response to Audit Processing Failures / Audit Storage Capacity	The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.			Yes	FHWA information system provides a warning to [Assignment: system owner and ISSM] within [Assignment: one (1) minute] when allocated audit record storage volume reaches [Assignment: at least 85%] of repository maximum audit record storage capacity.
DOT-AU-6	FHWA Clarification FHWA requires that system audit records from FHWA general support systems must be reviewed daily and audit records for FHWA major applications must be reviewed at least monthly.				
DOT-AU-6 Audit Review, Analysis, and Reporting	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].	Yes	Yes	Yes	FHWA must: a. Review and analyze information system audit records [Assignment: at least monthly] for indications of [Assignment: inappropriate or unusual activity]; and b. Reports findings to [Assignment: the FHWA ISSM].
DOT-AU-8 Time Stamps	The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and	Yes	Yes	Yes	FHWA information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	meets [Assignment: organization-defined granularity of time measurement].				Coordinated Universal Time (UTC) and meets [Assignment: within hundreds of milliseconds].
DOT-AU-9 Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Yes	Yes	Yes	The information systems restrict write access to audit logs so those whose activities are being logged can't change or delete the logs.
DOT-AU-9(2) Protection of Audit Information / Audit Backup on Separate Physical Systems / Components	The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited.			Yes	FHWA information system backs up audit records [Assignment: at least weekly] onto a physically different system or system component than the system or component being audited.
DOT-AU-9(3) Protection of Audit Information / Cryptographic Protection	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.			Yes	FHWA information system implements [FIPS 140-2 Level 3 validated] cryptographic mechanisms to protect the integrity of audit information and audit tools.
DOT-AU-10 Non-Repudiation	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].			Yes	FHWA information system must protect against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: configuration changes, audit log modification, malicious manipulation, forging the

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					identification of another user, spoofing mail messages]
DOT-AU-11 Audit Record Retention	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Yes	Yes	Yes	FHWA must retain audit records for [Assignment: For systems not requiring special accountability for access (such as user identification records generated according to preset requirements) retains at least eighteen (18) months and destroy when business use ceases; for systems requiring special accountability for access (such as user identification records associated with systems which are highly sensitive and potentially vulnerable) at least six (6) years and destroy after password is altered or user account is terminated, but longer retention is authorized if required for business use in accordance with Federal GRS 3.2 item 030 and 031 disposition authority.] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
CA-2 (2) Security Assessments	DOT Components must include as part of security control assessments [Parameter 1: organization-defined frequency], [Parameter 2: announced; unannounced], [Parameter 3: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Parameter 4: organization-defined other forms of security testing].			Yes	DOT Components must include as part of security control assessments [Assignment: Annual], [Assignment: announced], [Assignment: penetration testing];

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					[Assignment: and other vulnerability scanning as appropriate and cost-effective for the information system].
DOT-CA-3	FHWA Clarification Interconnections of an FHWA system that extend to systems outside of FHWA must be authorized by the Authorizing Official prior to allowing the interconnection.				
DOT-CM-2 Baseline Configuration	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Yes	Yes	Yes	FHWA must develop, document, and maintain under configuration control, a current ISSM approved baseline configuration of the information system.
DOT-CM-2(3) Baseline Configuration/ Retention Of Previous Configurations	The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.		Yes	Yes	FHWA must retain [Assignment: the last two previous versions of baseline configurations for the information system] to support rollback.
DOT-CM-2(7) Baseline Configuration/ Configure Systems, Components, or Devices for High-Risk Areas	The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.		Yes	Yes	No FHWA information systems, system components, or devices are to be taken outside the regions of the United States without formal authorization from the AO or ISSM.
DOT-CM-3	FHWA Clarification In FHWA, this control also applies to systems with a Federal Information Processing Standard (FIPS) 199 impact level of “low”.				
DOT-CM-3 Configuration Change Control	The organization: a. Determines the types of changes to the information system that are configuration-controlled;	Yes	Yes	Yes	System Owners with the approval of the ISSM must: a. Determine the types of changes to the information system that are configuration-controlled;

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].				b. Approve configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Document approved configuration-controlled changes to the system; d. Retain and review records of configuration-controlled changes to the system; e. Retains records of configuration-controlled changes to the information system for [Assignment: for a period of five (5) years. f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: The FHWA Configuration and Change Management Team as described in the FHWA Configuration and Change Management Process] that convenes [Assignment: weekly]; [Assignment: for all changes to FHWA information systems].
DOT-CM-4 Security Impact Analysis	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.		Yes	Yes	FHWA ISSM/ISSO must analyze/approve changes to the information system to determine

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					potential security impacts prior to change implementation.
DOT-CM-5(3) Access Restrictions For Change / Signed Components	The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.			Yes	FHWA information system prevents the installation of [Assignment: non-core technologies as identified within the FHWA enterprise architecture (EA)] without verification that the technology has been digitally signed using a certificate that is recognized and approved by FHWA.
DOT-CM-6	FHWA Clarification While DOT OCIO maintains a list of approved configuration baselines and deviations, the FHWA ISSM decides which baselines can be used within FHWA.				
DOT-CM-6 Configuration Settings	The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Yes	Yes	Yes	FHWA: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: FHWA-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: FHWA information system components]

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					based on [Assignment: DOT/FHWA operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with DOT/FHWA policies and procedures.
DOT-CM-7 Least Functionality	The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	Yes	Yes	Yes	FHWA: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services:[Assignment: <ul style="list-style-type: none"> Unsecure File Transfer Protocol; Telnet; Simple Network Management Protocol; Unrestricted Proxy Address Resolution Protocol messages Auto-execute].
DOT-CM-7(2) Least Functionality / Prevent Program Execution	The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].		Yes	Yes	The information system prevents program execution in accordance with [the [Assignment: FHWA Managing Software Inventory and Licenses policy regarding software program usage and restrictions].
DOT-CM-7(4) Least Functionality / Unauthorized	The organization: (a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information		Yes		FHWA: (a) Identifies in the FHWA information security plan [Assignment: software programs not authorized to execute on the

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Software / Blacklisting	system; and (c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].				information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [Assignment: on an annual basis].
DOT-CM-7(5) Least Functionality/A uthorized Software /Whitelisting	The organization: (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].			Yes	FHWA: (a) Identifies in the FHWA information security plan [Assignment: software programs that are authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: on an annual basis]
DOT-CM-8(3) Information System Component Inventory / Automated Unauthorized	The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].		Yes	Yes	FHWA: (a) Employs automated mechanisms [Assignment: continuously, using automated mechanisms with a maximum five-minute delay in detection] to detect the presence of unauthorized hardware, software, and firmware

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Component Detection					components within the information system; and (b) Takes the following actions when unauthorized components are detected: [notifies [Assignment: the FHWA ISSM]].
DOT-CM-9	FHWA Clarification NIST defines <i>configuration items</i> as the information system items (hardware, software, firmware, and documentation) to be configuration managed. FHWA subscribes to this definition.				
DOT-CM-11 User Installed Software	The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency].	Yes	Yes	Yes	FHWA: a. Employs DOT Established [Assignment: DOT Cybersecurity Compendium Policy] governing the installation of software by users; b. Enforces software installation policies through [Assignment: Administrative right privileges]; and c. Monitors policy compliance at [Assignment: near real-time basis].
DOT-CP-2 Contingency Plan	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency].	Yes	Yes	Yes	FHWA: a. Develops, documents, and disseminates to [Assignment: personnel responsible for addressing system contingencies and recovery and FHWA management responsible for the system, as deemed appropriate]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: annually]; and 2. Contingency planning procedures [Assignment: annually].
DOT-CP-7 Alternate Processing Site	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.		Yes	Yes	FHWA System Owners: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: FHWA-defined information system operations] for essential missions/business functions within [Assignment: the timeframe consistent with recovery time objectives identified in the information system business impact assessment] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
DOT-CP-8 Telecommunications Services	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.		Yes	Yes	System owner must establish alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: FHWA-defined information system operations] for essential missions and business functions within [Assignment: the timeframe consistent with recovery time objectives identified in the information system business impact assessment] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
DOT-IA-3 Device Identification and Authentication	The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.		Yes	Yes	The information system uniquely identifies and authenticates [Assignment: Servers, routers, switches and other network devices] before establishing a [local, remote, or network] connection.

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-IA-4 Identifier Management	The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].	Yes	Yes	Yes	FHWA manages information system identifiers by: a. Receiving authorization from [Assignment: system owner] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: a minimum of 365 days]; and e. Disabling the identifier after [Assignment: after 90 days of inactivity for low impact level systems and after 60 days of inactivity for Moderate and 30 days of inactivity for High impact level systems.].
DOT-IA-5 Authenticator Management	The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;	Yes	Yes	Yes	FHWA manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the DOT; c. Ensuring that authenticators

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.				have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: every 60 days]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
DOT-IA-5(1) Authenticator Management / Password-	The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and	Yes	Yes	Yes	The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: a

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Based Authentication	special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.				minimum of twelve (12) characters and must contain a combination of: - 1 uppercase character - 1 lowercase character - 1 numeric character - 1 special character.]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: at least one (1) or as determined by the system]; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: one (1) day minimum and 60 day maximum]; (e) Prohibits password reuse for [Assignment: 24] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.
DOT-IA-5(3) Authenticator Management / In-Person Or Trusted Third-Party Registration	The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].		Yes	Yes	FHWA follows DOT and Federal policies and guidelines for the registration process of each type of authenticator.

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-IA-5(11) Authenticator Management / Hardware Token-Based Authentication	The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].	Yes	Yes	Yes	The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: HSPD-12 token quality requirements].
DOT-IA-7 Cryptographic Module Authentication	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Yes	Yes	Yes	FHWA information system implements mechanisms for authentication to a cryptographic module that meet the requirements of FIPS 140-2, additional applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
DOT-IA-8 Identification and Authentication (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Yes	Yes	Yes	The information system uniquely identifies and authenticates non-organizational users (through ORC Level 2 credentials, approved User-ID and passwords, or other mechanisms approved by the AO).
DOT-IA-8(2) Identification and Authentication / Acceptance of Third-Party Credentials	The information system accepts only FICAM-approved third-party credentials.	Yes	Yes	Yes	FHWA information system must use FICAM-approved third-party credentials when third party credentials are required.
DOT-MA-3(3) Maintenance Tools / Prevent	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment;			Yes	FHWA prevents the unauthorized removal of maintenance equipment containing FHWA information by: (a) Verifying that there is no FHWA

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Unauthorized Media	(b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.				information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: FHWA ISSM] explicitly authorizing removal of the equipment from the facility. Additionally, FHWA ensures that the maintenance equipment is either sanitized or destroyed via the Media Sanitation Guide located in Appendix F of this document.
DOT-MP-2	FHWA Clarification FHWA information owners must restrict access to FHWA information stored on digital and non-digital media to only those individuals with a need to know. In order to restrict access, logical and/or physical measures must be employed.				
DOT-MP-2 Media Access	The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Yes	Yes	Yes	FHWA access to [Digital and non-digital media (see section 2.11 of the FHWA Cybersecurity Program Handbook for a description of digital and non-digital media)] to [Individuals with the “need to know”]
DOT-MP-2.a Media Access	System Owners must authorize, document, and maintain an inventory of media that contains sensitive data. This information must be retained for a period of [organization defined time period].	Yes	Yes	Yes	System Owners must authorize, document, and maintain an inventory of media that contains sensitive data. This information must be retained for a period of [six (6) months after the media retention period has expired].

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-MP-2.d	FHWA Clarification All FHWA employees and contractors cannot process or store FHWA information in digital form on non-DOT/non-FHWA issued media unless approved in writing by the FHWA ISSM. This includes but is not limited to the digital media types described at the beginning of section 2.11 of this handbook. Please note that non-DOT issued media includes the hard-drive of a personally owned desktop or laptop computer, personally owned tablet computers including iPads, personally owned cell phones that are not included in DOT’s mobile device management program (MDM) which includes the installation of the Good Software on the device. Furthermore, when using flash/thumb drives or external hard drives only self-encrypting drives can be used. FHWA StaffNet contains information on makes and models of approved self-encrypting drives.				
DOT-MP-3 Media Marking	The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].		Yes	Yes	System Owners must: a. Mark, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt [backup tapes] from marking as long as the exempted items remain within [DOT/FHWA limited access controlled areas].
DOT-MP-3.b	System Owners must document and maintain a record of media which has been sanitized and/or destroyed for the purpose of disposal for a period of [organization defined].		Yes	Yes	System Owners must document and maintain a record of media which has been sanitized and/or destroyed for the purpose of disposal for a period of [18 months after media is destroyed but longer retention is authorized if required for business use].
DOT-MP-4 Media Storage	The organization:		Yes	Yes	System Owners must: a. Physically control and securely

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.				store [Assignment: magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks] within [Assignment: access controlled data center and office areas, locked cabinets, safes, and other areas where access is restricted to those with a “need to know”] b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
DOT-MP-6(3) Media Sanitation	The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].			Yes	FHWA applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: when devices are reassigned for reuse].
DOT-PE-3 Physical Access Control	The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];	Yes	Yes	Yes	FHWA: a. Enforces physical access authorizations at [Assignment: entry/exit points to the facility where FHWA's information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Assignment: HSPD-

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	<p>c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;</p> <p>d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];</p> <p>e. Secures keys, combinations, and other physical access devices;</p> <p>f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and</p> <p>g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.</p>				<p>12 physical access control systems/devices and/or guards];</p> <p>b. Maintains physical access audit logs for [entry/exit points];</p> <p>c. Provides [Assignment: physical security safeguards] to control access to areas within the facility officially designated as publicly accessible;</p> <p>d. Escorts visitors and monitors visitor activity [Assignment: for circumstances requiring visitor escorts and monitoring];</p> <p>e. Secures keys, combinations, and other physical access devices;</p> <p>f. Inventories [FHWA physical access devices] every [Assignment: at least annually]; and</p> <p>g. Changes combinations and keys [Assignment: every two (2) years] and/or when keys are lost, combinations are compromised, or individuals are transferred or employment terminated.</p>
DOT-PE-10 Emergency Shutoff	<p>The organization:</p> <p>a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;</p> <p>b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and</p> <p>c. Protects emergency power shutoff capability from unauthorized activation.</p>		Yes	Yes	<p>FHWA:</p> <p>a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;</p> <p>b. Places emergency shutoff switches or devices in [Assignment: an easily seen and accessible</p>

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					location preferably near the exit] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.
DOT-PE-14 Temperature and Humidity Controls	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].	Yes	Yes	Yes	FHWA: a. Maintains temperature and humidity levels within the facility where FHWA's information system resides at [Assignment: the levels specified by the vendor for the information system hardware components, including but not limited to, servers, telecommunications equipment, and storage devices]; and b. Monitors temperature and humidity levels [Assignment: continuously].
DOT-PE-16 Delivery and Removal	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	Yes	Yes	Yes	FHWA authorizes, monitors, and controls [Assignment: IT equipment such as servers, telecommunications equipment, storage devices and other IT devices.] entering and exiting the facility and maintains records of those items.
DOT-PE-17 Alternate Work Site	The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and		Yes	Yes	The organization: a. Employs [Assignment: for FHWA employees: Security requirements outlined in the <i>FHWA Order 3620.1</i> , Telework Program, dated January

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.				27, 2010; For contractor's security requirements outlined in their contract or identified by the Contracting Officer's Representative.] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
DOT-PE-18	FHWA Clarification FHWA organizations may not construct or create new data centers. Furthermore, FHWA IT information systems must be in a hosting facility or data center approved by the DOT CIO. The process to get a hosting facility or data center approved by the DOT CIO requires the approval of the FHWA ISSM who will obtain the DOT CIO approval.				
DOT-PL-2 System Security Plan	The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;	Yes	Yes	Yes	FHWA: a. Develops a security plan for the information system that: 1. Is consistent with the DOT/FHWA enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	<p>b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];</p> <p>c. Reviews the security plan for the information system [Assignment: organization-defined frequency];</p> <p>d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and</p> <p>e. Protects the security plan from unauthorized disclosure and modification.</p>				<p>rationale;</p> <p>5. Describes the operational environment for the information system and relationships with or connections to other information systems;</p> <p>6. Provides an overview of the security requirements for the system;</p> <p>7. Identifies any relevant NIST defined overlays (i.e., specialized control sets) applicable to the FHWA information system;</p> <p>8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and</p> <p>9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;</p> <p>b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: the FHWA ISSM/ISSO];</p> <p>c. Reviews the security plan for the information system [Assignment: annually or the result of a significant change];</p> <p>d. Updates the plan to address changes to the information system/environment of operation</p>

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.
DOT-PL-2(3) System Security Plan Plan / Coordinate with other Organizational Entities	The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.		Yes	Yes	The organization plans and coordinates security-related activities affecting the information system with [Assignment: FHWA AO, ISSM, ISSO, System Owner, System Administrators (Support Personnel), Disaster Recovery Team, FHWA SOC, and/or other affected parties as applicable] before conducting such activities in order to reduce the impact on other organizational entities.
DOT-PL-4 Rules of Behavior	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.	Yes	Yes	Yes	FHWA: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed or electronic acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					information and the information system; c. Reviews and updates the rules of behavior [Assignment: must be review annually and updated as needed based upon the review]; and d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and acknowledge the new rules when the rules are revised/updated.
DOT-PS-2 Position Risk Designation	The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency].	Yes	Yes	Yes	FHWA: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: When new positions and descriptions are added and upon DOT guidance updates].
DOT-PS-3 Personnel Screening	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].	Yes	Yes	Yes	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: DOT 1630.2C <i>Personnel Security Management</i>].
DOT-PS-4 Personnel Termination	The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period];	Yes	Yes	Yes	FHWA, upon termination of individual employment: a. Disables information system

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].				access within [Assignment: - immediately on Day of Separation]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts an exit interview or survey that includes a discussion of [Assignment: FHWA information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: system owner] within [Assignment: upon termination of an individual].
DOT-PS-4(2) Personnel Termination / Automated Notification	The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.			Yes	FHWA employs automated mechanisms to notify [Assignment: FHWA Human Resources for Federal employees or the COR for contractors] upon termination of an individual.
DOT-PS-5 Personnel Transfer	The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];	Yes	Yes	Yes	FHWA: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].				b. Initiates [Assignment: appropriate actions as defined within the Process of the request thru Service Request Management (SRM) automated system and/or other established process] within [Assignment: at least three (3) business days]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: FHWA Human Resources for Federal employees or the COR for contractors] within [Assignment: at least two weeks].
DOT-PS-6 Access Agreements	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].	Yes	Yes	Yes	FHWA: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: review at least annually and update as needed]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access. Can be a digital signature or other electronic notifications.

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: at least annually].
DOT-PS-6.b Access Agreements	DOT Components must retain record of access agreements in accordance with approved retention schedule [Refer to Appendix A for retention schedule].	Yes	Yes	Yes	FHWA must retain record of access agreements in accordance with approved retention schedule [Assignment: established by National Archives and Records Administration General Records 3.2, item 030 and 031, for systems not requiring special accountability for access, FHWA retains record of access agreements for 18 months and destroys when business use ceases. For systems requiring special accountability for access FHWA retains record of access agreements for 6 years and destroys after password is altered or user account is terminated, but longer retention is authorized if required for business use].
DOT-PS-8.a	FHWA Clarification Refer to DOT control DOT-AC-2.i in Section 2.2 of this handbook for a list of reasons FHWA may revoke the access of a user to DOT/FHWA information systems.				
DOT-RA-5	FHWA Clarification It is FHWA's practice to scan our general support systems at least weekly.				
DOT-SA-3	FHWA Clarification Appendix E of this document describes the FHWA System Development Life Cycle (SDLC) and outlines the security activities that take place at each of the five phases of the SDLC.				

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
DOT-SA-3 System Development Lifecycle	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	Yes	Yes	Yes	FHWA: a. Manages the information system using [Assignment: an SDLC process that is compliant with the SDLC contained in appendix E of this CSP] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.
DOT-SA-4	FHWA Clarification Production data whether sensitive or non-sensitive cannot be used on non-production systems without the approval of the FHWA ISSM.				
DOT-SA-4 Acquisition Process	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation;	Yes	Yes	Yes	FHWA includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.				mission/business needs: a. Security functional requirements including DOT specified languages for Cloud Service Providers. b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria. FHWA follows the DOT Federal Acquisition Regulations (FAR) and the Department of Transportation Acquisition Regulations (TAR).
DOT-SA-4(1) Acquisition Process Functional Properties Of Security Controls	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.		Yes	Yes	FHWA requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed in an information system technical architecture document or other appropriate documentation.
DOT-SA-4(2) Acquisition Process Design/ Implementation	The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or		Yes	Yes	FHWA requires the developer of the information system, system component, or information system service to provide design and implementation information for

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Information For Security Controls	hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].				the security controls to be employed that includes: [security-relevant external system interfaces, high-level design and source code or hardware schematics; [Assignment: utilizing software development procedures that are in compliance with the SDLC contained in Appendix E of this CSP] at [Assignment: sufficient detail to permit analysis and testing of the controls].
DOT-SA-4(9) Acquisition Process Functions / Ports / Protocols / Services In Use	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.		Yes	Yes	FHWA requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for FHWA use [in accordance with an SDLC process that is compliant with the SDLC contained in appendix E of this CSP]].
DOT-SA-8 Security Engineering Principles	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.		Yes	Yes	FHWA applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system in accordance with the principles outlined in the Appendix E of this handbook.
DOT-SA-9 External	The organization: a. Requires that providers of external information system services	Yes	Yes	Yes	FHWA: a. Requires that providers of

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Information System Services	<p>comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;</p> <p>b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and</p> <p>c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.</p>				<p>external information system services comply with organizational information security requirements and employ [Assignment: DOT/FHWA security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;</p> <p>b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and</p> <p>c. Employs [Assignment: DOT/FHWA processes, methods, and techniques as prescribed within this handbook] to monitor security control compliance by external service providers on an ongoing basis.</p>
DOT-SA-10 Developer Configuration Management	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <p>a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];</p> <p>b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];</p> <p>c. Implement only organization-approved changes to the system, component, or service;</p> <p>d. Document approved changes to the system, component, or service</p>		Yes	Yes	<p>FHWA requires the developer of the information system, system component, or information system service to:</p> <p>a. Perform configuration management during system, component, or service [design, development, implementation, and operation];</p> <p>b. Document, manage, and control the integrity of changes to</p>

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].				[Assignment: the FHWA Configuration and Change Management Process or other ISSM approved Configuration and Change Process]; c. Implement only FHWA-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: FHWA ISSM/ISSO].
DOT-SA-12 Supply Chain Protection	The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.			Yes	FHWA protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: at a minimum, but not limited to: maintenance agreements, configuration management, physical and logical access controls, separation of duties, updates for current versions and patch management] as part of a comprehensive, defense-in-breadth information security strategy.
DOT-SA-16 Developer	The organization requires the developer of the information system, system component, or information system service to provide			Yes	FHWA requires the developer of the information system, system

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
Provided Training	[Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.				component, or information system service to provide [Assignment: FHWA ISSM approved training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.
DOT-SA-17 Developer Security Architecture And Design	The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.			Yes	FHWA requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the FHWA's security architecture which is established within and is an integrated part of the FHWA's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
DOT-SC-7 Boundary Protection	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components	Yes	Yes	Yes	The information system: a. Monitors and controls communications [utilizing the DHS Trusted Internet Connection (TIC)]

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.				at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [logically] separated from internal DOT/FHWA networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a DOT/FHWA security architecture.
DOT-SC-7(3) Boundary Protection Access Points	The organization limits the number of external network connections to the information system.		Yes	Yes	FHWA limits the number of external network connections to the information system to two (2).
DOT-SC-7(4) Boundary Protection External Telecommunications Services	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.		Yes	Yes	FHWA: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: at

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					least annually] and removes exceptions that are no longer supported by an explicit mission/business need.
DOT-SC-7(21) Boundary Protection Isolation Of Information System components	The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].			Yes	FHWA employs boundary protection mechanisms to separate [Assignment: information system components] supporting [Assignment: FHWA missions and/or business functions].
DOT-SC-8(1) Transmission Confidentiality And Integrity Cryptographic Or Alternate Physical Protection	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].		Yes	Yes	The information system implements cryptographic mechanisms to [prevent unauthorized disclosure of information and detect changes to information] during transmission unless otherwise protected by [Assignment: a protected Distribution System (PDS) approved by the FHWA ISSM].
DOT-SC-12 Cryptographic Key Establishment And Management	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Yes	Yes		FHWA establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: encryption that is NIST FIPS 140-2 validated].
DOT-SC-13 Cryptographic Protection	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Yes	Yes	Yes	The information system implements [Assignment: Encryption for data at rest and in transit that is compliant with (FIPS) 140-2 standard] in accordance with applicable federal

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					laws, Executive Orders, directives, policies, regulations, and standards.
DOT-SC-15 Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	Yes	Yes	Yes	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: no exception]; and b. Provides an explicit indication of use to users physically present at the devices.
DOT-SC-18	FHWA Clarification FHWA controls the use of Mobile code and mobile technologies by requiring that System Owners obtain written approval from the FHWA ISSM for the use of mobile code and mobile code technologies before they are deployed in FHWA information systems. Furthermore, the use of mobile code and mobile code technologies for an information system must be explicitly identified and completely documented in the security plan or technical architecture document for the information system.				
DOT-SC-18 Mobile Code	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.		Yes	Yes	FHWA: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system. Guidance: Please see FHWA Clarification above
DOT-SC-19	FHWA Clarification				

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	FHWA non-HQ organizations implementing Voice Over Internet Protocol (VOIP) phone systems must obtain approval from FHWA’s Office of Information Technology Services (OITS) prior to purchasing a system. Once the system has been acquired it must be configured in accordance with DOT’s COE and FHWA requirements.				
DOT-SC-19 Voice Over Internet Protocol	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system		Yes	Yes	FHWA: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system Guidance: Please see FHWA Clarification above
DOT-SC-23 Session Authenticity	The information system protects the authenticity of communications sessions.		Yes	Yes	The information system protects the authenticity of communications sessions.
DOT-SC-28 Protection Of Information At Rest	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].		Yes	Yes	The information system protects the [confidentiality] of [Assignment: Controlled Unclassified Information (CUI) at rest].
SI-4 Information System Monitoring	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and		Yes	Yes	FHWA System Owners must: a. Monitor the information system to detect: 1. Attack and indicators of potential attacks in accordance with [Assignment: the information system audit capability to detect abnormal user activities]; and

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
	<p>(ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;</p> <p>d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</p> <p>e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;</p> <p>f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and</p> <p>g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].</p>				<p>2. Unauthorized local, network, and remote connections;</p> <p>b. Identify unauthorized use of the information system through [Assignment: system-defined techniques and methods];</p> <p>c. Deploy monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;</p> <p>d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</p> <p>e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;</p> <p>f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive</p>

Appendix A: FHWA Requirements Established for the DOT Cybersecurity Compendium Workbook

Policy ID / Control	Description	FIPS 199 Impact Level			FHWA Defined Parameters
		L	M	H	
					Orders, directives, policies, or regulations; and g. Provide [Assignment: system-defined information system monitoring information] to [Assignment: FHWA ISSM/ISSO] [as needed; [Assignment: continuously in real-time]].
SI-4 (22) Information System Monitoring, Unauthorized Network Services	The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles]].	Yes	Yes	Yes	FHWA information system prohibits and detects network services that have not been authorized or approved by [Assignment: DOT and ISSM approval process] and alerts [Assignment: FHWA CIO and/or DOT CSIRC]
SI-5 Security Alerts, Advisories, and Directives	The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Yes	Yes	Yes	The DOT CSIRC must: a. Receive information system security alerts, advisories, and directives from designated internal and external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to [Assignment: DOT SOC as appropriate]; and d. Implement security directives in accordance with established time frames, or notify [FHWA] of the degree of noncompliance.

APPENDIX - B ACRONYMS

Acronyms and Abbreviations

AC	Access Control
AECM	Automated Enterprise Continuous Monitoring
AO	Authorizing Official
AT	Security Awareness and Training
AU	Audit and Accountability
BDR	Budget Data Request
BIA	Business Impact Analysis
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CM	Continuous Monitoring
CO	Contracting Officers
COE	Common Operating Environment
COTS	Commercial Off-The-Shelf
CP	Contingency Planning
CPIC	Capital Planning and Investment Control
CSIRC	Computer Security Incident Response Center
CSP	Cybersecurity Program
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposure
DISA	Defense Information Systems Agency
DOT	Department of Transportation
EA	Enterprise Architecture
FHWA	Federal Highway Administration
FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
GSS	General Support System
HAAM	Office of Acquisitions Management
HQ	Headquarters

HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IDS	Intrusion Detection System
IO	Information Owner
IPS	Intrusion Protection System
IR	Incident Response
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITD	Information Technology Division
MA	Maintenance
MDM	Mobile Device Management
MP	Media Protection
NIST	National Institute of Standards and Technology
OITS	Office of Information Technology Services
OMB	Office of Management and Budget
PE	Physical and Environmental Protection
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SDLC	System Development Life Cycle
SI	System and Information Integrity
SO	System Owner
SOC	Security Operations Center
SP	Special Publication
TIC	Trusted Internet Connection
UTC	Coordinated Universal Time
VOIP	Voice Over Internet Protocol

APPENDIX - C ISSM DESIGNATION LETTER

Memorandum

Subject: Designation of the Information System Security Manager

Date: MAR 31 2014

From: Sarah J. Shores
Associate Administrator for Administration
Federal Highway Administration

To: Cheryl Ledbetter

Cc: Joe Albaugh, DOT Chief Information Security Officer

In accordance with DOT Cybersecurity Policy DOT Order 1351.37, I am designating you the Information System Security Manager (ISSM) for Federal Highway Administration.

Responsibilities

The responsibilities for this position, as described in DOT Order 1351.37, are outlined here for your reference. If DOT Order 1351.37 is updated, the current version of DOT Order 1351.37 and the responsibilities assigned to the ISSM role supersede those listed below.

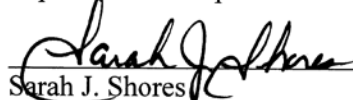
- a) Overseeing the Federal Highway Administration Cybersecurity Program;
- b) Ensuring the Federal Highway Administration CIO and DOT CISO are kept apprised of all pertinent matters involving the security of information systems;
- c) Ensuring information security-related decisions and information, including updates to this Departmental Cybersecurity Policy and the supplemental Departmental Cybersecurity Compendium, are distributed to the ISSOs and other appropriate persons within this organization;
- d) Ensuring DOT guidance is followed to identify, categorize and report an accurate information systems inventory for the Federal Highway Administration and that this inventory is reported and maintained in accordance with DOT policy and guidance contained within the Departmental Cybersecurity Compendium;
- e) Validating all Federal Highway Administration information system security reporting;
- f) Managing information security resources including oversight and review of security requirements in funding documents;
- g) Testing, periodically, the security of implemented information systems;
- h) Implementing and managing a POA&M process for remediation;
- i) Serving as the primary liaison for the Federal Highway Administration CIO to the Federal Highway Administration's AOs, information system owners, common control providers, and ISSOs;

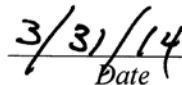
- j) Ensuring each system has an ISSO appointed by the Federal Highway Administration and that this appointment is documented;
- k) Ensuring weekly incident reports are forwarded to the DOT CISO;
- l) Acknowledging receipt of alerts, advisories, and bulletins sent by the DOT CSIRC and ensuring these messages are routed to the appropriate Federal Highway Administration personnel;
- m) Providing the DOT CSIRC the current list of Federal Highway Administration personnel that are authorized to interact with the DOT CSIRC to include, at a minimum, the Federal Highway Administration CIO, Federal Highway Administration ISSM and Federal Highway Administration ISSOs;
- n) Ensuring adherence to DOT-approved Secure Configuration Baselines defined in the Departmental Cybersecurity Compendium;
- o) Developing and publishing procedures necessary to implement the requirements of DOT information security policy within the appropriate Federal Highway Administration;
- p) Implementing Departmental information security policies, procedures, and control techniques to address all applicable requirements;
- q) Ensuring personnel with significant responsibilities for cybersecurity are identified as specified in the Departmental Cybersecurity Compendium and that annual training is completed, tracked, and reported;
- r) Leading Federal Highway Administration cybersecurity and incident response programs;
- s) Promoting proper Cybersecurity practices;
- t) Supporting the DOT CISO in the implementation of the DOT Cybersecurity Program;
- u) Fostering communication and collaboration among DOT security stakeholders to share knowledge and to better understand threats to DOT information;
- v) Providing information about the Federal Highway Administration cybersecurity policies to management and throughout DOT;
- w) Providing advice and assistance to other organizational personnel concerning the security of sensitive data and of critical data processing capabilities;
- x) Advising the Federal Highway Administration CIO about security breaches in accordance with the security breach reporting procedures developed and implemented by this organization;
- y) Disseminating information on potential security threats and recommended safeguards;
- z) Ensuring roles with significant security responsibilities are identified and documented per the Departmental Cybersecurity Compendium;
- aa) Conducting security education and awareness training needs assessments to determine requirements and leveraging available DOT-wide resources to satisfy these requirements. When DOT-wide available resources do not meet requirements, coordinating with Federal Highway Administration CIO and program officials to identify cost effective solutions for meeting mandatory requirements in accordance with DOT awareness and

- training policy specified in the Departmental Cybersecurity Compendium;
- bb) Providing feedback obtained from users of DOT-wide training resources to the DOT CISO to aid in improving the content and delivery of DOT-provided training;
 - cc) Assisting System Owners in establishing and implementing the required security safeguards to protect computer hardware, software, and data from improper use or abuse;
 - dd) Communicating requirements for personnel clearances and position sensitivity determinations necessary for access to information systems with the appropriate office;
 - ee) Ensuring Federal Highway Administration-wide implementation of DOT and Federal Highway Administration policies and procedures that relate to Cybersecurity and incident response;
 - ff) Collaborating with the DOT Privacy Breach Response Team (BRT) Coordinator when engaging the Federal Highway Administration POC for information collection and clarification, and sitting on the DOT Privacy BRT while the breach is under investigation;
 - gg) Immediately notifying the Federal Highway Administration Privacy Officer and DOT Privacy Officer when privacy-related or PII incidents are suspected or reported within the Federal Highway Administration;
 - hh) Establishing, documenting, and enforcing requirements and processes for granting and terminating all administrative privileges including, but not limited to, servers, domains, and local workstations auditing these processes for effectiveness in accordance with policy specified in the Departmental Cybersecurity Compendium;
 - ii) Ensuring enterprise security tools are leveraged to their fullest extent and ensuring all security tools that the Federal Highway Administration selects and implements conforms to the DOT Cybersecurity continuous monitoring technical architecture and standards;
 - jj) Ensuring Federal Highway Administration incidents are reported to the DOT CSIRC in accordance with DOT Cybersecurity policies and DOT CSIRC procedures;
 - kk) Completing mandatory annual specialized information security training; and
 - ll) Completing additional responsibilities that are described within the DOT Cybersecurity Compendium and its associated appendices.

Certification

I certify that you are a Federal employee and that you possess the necessary knowledge and skills to perform the responsibilities associated with the role.


Sarah J. Shores
Chief Information Officer


Date

ISSM Designation

Acceptance

I acknowledge assignment of the ISSM role and understand the responsibilities associated with the position.

Cheryl Ledbetter
Cheryl Ledbetter

3/31/14
Date

APPENDIX - D FHWA IT SECURITY INCIDENT REPORTING PROCEDURES

FHWA IT SECURITY INCIDENT REPORTING PROCEDURES

REPORTING INCIDENTS

Purpose:

As a Component of the Department of Transportation, FHWA is required to establish information technology (IT) security incident reporting procedures. The purpose of these procedures is to establish a standard, FHWA-wide method for reporting and acting on security incidents.

What should I report?

The Federal Computer Incident Response Center (FedCIRC) defines an incident as an event violating an explicit or implied security policy. The following types of events or activities are widely recognized as being in violation of a typical security policy. These activities include but are not necessarily limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the transmission, processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Lost or stolen Information Technology (IT) equipment or devices
- These events can manifest themselves in many ways. Specific examples of incidents include but are not limited to:
 - Lost, stolen, or missing IT equipment including but not limited to: smartphones including iPhones, Blackberries, laptops, workstations, external hard drives, flash drives, thumb drives, memory sticks
 - Suspicious entries in system or network accounting such as a UNIX user obtaining root access without going through the normal sequence necessary to obtain this access
 - Accounting discrepancies such as an 18-minute gap in the accounting log in which no entries whatsoever appear
 - Unsuccessful logon attempts
 - Unexplained new user accounts
 - Unexplained new files or unfamiliar file names
 - Unexplained modifications to file lengths or dates especially in system executable files
 - Unexplained modification or deletion of data
 - Denial of service or inability of one or more users to login to an account
 - System crashes
 - Poor system performance or erratic behavior of a system
 - Unauthorized operation of a program or sniffer device to capture network traffic
 - Use of attack scanners or programs
 - Remote requests for information about systems and/or users
 - Social engineering attempts
 - Unusual time of usage (more security incidents occur during non-working hours than any other time)
 - Unusual usage patterns such as programs being compiled in the account of a user who does not know how to program)
 - Spam, scams or other suspicious emails received at your DOT provided email address.

You should report any activity that you feel meets the criteria for a security incident, or that is suspicious in nature. Even if you are not sure whether or not an actual incident has taken place

you should still report your suspicions that one might have taken place (Note: ***It is better to report and if necessary, withdraw the report then not report at all!***)

If I find an incident in progress, are there any immediate actions I should take?

If you believe that you have discovered an ongoing incident, your first response may be to try to stop the incident by unplugging or rebooting the system that is under attack. If possible, DO NOTHING to the workstation or system until the Information Technology Shared Services (ITSS) Service Desk, COE Remediation staff or FHWA IT Security Staff respond.

When do I report?

All incidents (actual or suspected) must be reported immediately.

How do I report an incident?

- Contact the DOT Security Operations Center (DOT SOC) by phone at 571-209-3080 or by email at 9-AWA-SOC@faa.gov for all incidents except spam, scams or other suspicious emails. When reporting to the DOT SOC make sure that you contact the FHWA ISSM Cheryl Ledbetter at 202-366-9030 or cheryl.ledbetter@dot.gov
- Report spam, scams, or suspicious email to the DOT SOC by email at 9-AWA-SOC@faa.gov with a copy to spamabuse@dot.gov and ITSECUREFHWA@dot.gov. Rather than forwarding the original email to these addresses, include it as an attachment.
- Please provide as much information as possible when reporting an incident. Remember if the incident you are reporting involves your PC or workstation or any system you administer or the data stored on it, if possible, DO NOTHING until you are contacted by an FHWA ISSM/ISSO, the DOT SOC, the FHWA IT Security Operations Team or the COE Remediation technicians.

APPENDIX - E FHWA INFORMATION SECURITY IN THE SYSTEM DEVELOPMENT LIFE CYCLE

FHWA INFORMATION SECURITY IN THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE

1.0 Purpose

The purpose of these procedures is to establish standard, FHWA-wide security activities that occur within a system development lifecycle (SDLC) methodology.

2.0 FHWA Software Development Lifecycle

The FHWA SDLC contains five phases:

- **Initiation** — begins after the Phase II Investment Review Board (IRB)'s approval to implement recommended solution for a system, and during the defining system security requirement
- **Acquisition/Development** — during this phase, the system is purchased, designed, programmed, developed, or otherwise constructed
- **Implementation/Assessment** — the system is prepped and made ready for production during which security testing is performed
- **Operation and Maintenance** — during this phase, the system is operating within the production environment, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced
- **Disposal** — this phase begins when the decision is made to terminate the system, activities conducted ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies

Each phase includes a minimum set of security tasks in each of the above SDLC phases needed to effectively incorporate security into the system.

3.0 Incorporating Security into the SDLC

The following identifies and describes the major security activities in each phase.

3.1 Initiation Phase

- Define security requirements
 - Categorize the Information System via the Federal Information Processing Standard (FIPS) Publication 199
 - Perform Business Impact Analysis (BIA)
 - Perform Privacy Threshold Analysis (PTA).
 - In the event that it is determined that the system contains privacy information perform the PIA and create the system of records notice (SORN) if indicated by the PIA.
- Perform E-Authentication Risk Assessment
- Initiate Security Plan Document
 - Document FIPS 199 Categorization
 - Document Security requirements

3.2 Acquisition/Development Phase

- Begin Risk Assessment
- Select and Document Security Controls within the Security Plan from NIST SP 800-53 Revision 4

- Begin Technical Architecture Document
- Engineer in Security
 - Implement security controls as stipulated by the security plan.
- Develop Security Documentation
 - Additional security documentation supporting the security plan (i.e., Contingency plan, configuration management plan, etc.)

3.3 Implementation / Assessment Phase

- Complete Risk Assessment
- Perform System Testing via the Security Controls Assessment Plan.
- Develop Security Assessment Report
 - Security Authorization Package, which includes the Security Assessment Report, the Plan of Action and Milestone (POA&M), and the updated Security Plan.
 - Assessment results are shared with system owner, FHWA ISSM, system administrator, and developers.
- Authorize the Information System
 - Security Authorization Decision, documented and transmitted from Authorizing Official to System Owner and ISSM
 - Final Security Authorization Package

3.4 Operations and Maintenance Phase

- Perform Configuration Management and Control
 - Security evaluations of requested system changes
 - Updated security documentation (Security Plan, POA&M status)
- Conduct Continuous Monitoring
 - Documented results of continuous monitoring
 - Continuous monitoring should be adjusted as risk levels fluctuate and security controls are modified, added, and discontinued.
 - POA&M review
 - Security reviews, metrics, measures, and trend analysis
 - Updated security documentation and security re-authorization decision, as necessary

3.5 Disposal Phase

- Disposition of System Information
 - Safeguard vital system information
 - Migrate data processed by the system to a new system if needed
 - Preserve data in accordance with applicable records management regulations and policies as required
 - Sanitize media as necessary
- Dispose of Hardware and Software
 - Maintain disposition records for hardware and software. These records may include lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.
 - Update system and component inventories.
- Closure of System

- Generate documentation verifying system closure, including final closure notification to the authorizing official, system owner, ISSM, and program manager.

4.0 Roles and Responsibilities

The following matrix defines and documents information system security roles and responsibilities throughout the system development life cycle.

Roles	Responsibilities
System Owner	All phases of the SDLC. Also, responsible for the overall security and privacy of the system throughout its initiation through disposal including development and maintenance of security documentation.
ISSM	Ensures that required security controls are implemented and maintained throughout the life of the system.
Privacy Officer	In conjunction with the system owner ensures adequate attention to privacy is achieved and maintained during all phases of the SDLC.
Authorizing Official	Authorizes the system to operate and accepts any residual risk during all phases of the SDLC.
Developer/Programmer/System Administrators	Design, implement and maintain adequate security measures for the system. Maintain adequate system documentation including documentation of security controls. Ensure adequate security is maintained throughout the life of the system.

APPENDIX - F FHWA MEDIA SANITIZATION REQUEST PROCEDURES

Federal Highway Administration (FHWA) Media Sanitization Request Procedures

OFFICE OF INFORMATION TECHNOLOGY SERVICES
Information Technology Strategic Objective

November 2017



U.S. Department
of Transportation

**Federal Highway
Administration**

Record of Change

The following changes have been incorporated into FHWA CSP Handbook.

[illegible]

Table of Contents

CHAPTER ONE

1.0 PURPOSE OF DOCUMENT	F-1
1.1 SCOPE AND APPLICATION	F-1
1.2 REFERENCE DOCUMENT(S)	F-1

CHAPTER TWO

2.0 PREPARE AND SUBMIT MEDIA SANITIZATION REQUEST FORM	F-1
2.1 PACKAGE AND SUBMIT REQUEST FORM AND MEDIA TO BE SANITIZED	F-1
2.3 SANITIZATION OF MEDIA	F-2

APPENDIX A MEDIA SANITIZATION REQUEST FORM	FORM-1
--	--------

OVERVIEW

MEDIA ASSURANCE

PURPOSE OF DOCUMENT

This document describes the process that FHWA employees and contractors follow when they need to have digital media such as hard drives and backup tapes sanitized prior to their being discarded or excessed.

SCOPE AND APPLICATION

This procedure applies to FHWA IT computer specialists in the field, at Federal Lands Offices, Headquarters (HQ) and any other FHWA employees and contractors handling the decommission or excessing of FHWA computer equipment including digital media.

REFERENCE DOCUMENT(S)

Departmental Cybersecurity Compendium, Supplement to DOT Order 1351.37 Departmental Cybersecurity Policy – Media Protection (MP)

MEDIA SANITIZATION REQUEST PROCEDURE

This procedure describes the actions to be taken to request sanitization of digital media that has been decommissioned or is otherwise determined to be of no further operational use. The actual sanitization is performed by FHWA HQ personnel assigned the responsibility for media sanitization.

PREPARE AND SUBMIT MEDIA SANITIZATION REQUEST FORM

To request media sanitization the requesting individual must complete sections I and II of the Media Sanitization Request Form. A copy of the form and instructions for completing the form are included in Appendix A of this document.

Please ensure that except for signature fields all fields are typed or printed legibly. The media to be sanitized must be fully identified on the form. Section II of the form allows up to 5 individual requests. Additional forms are required if there are more than 5 individual request.

PACKAGE AND SUBMIT REQUEST FORM AND MEDIA TO BE SANITIZED

Package the media and the Media Sanitization Request Form together and send or deliver this form and the media to the FHWA Information Systems Security Manager (ISSM) at:

Ms. Cheryl Ledbetter

Department of Transportation
Federal Highway Administration (HAIM 42)
FHWA Information Systems Security Manager (ISSM)
Room E76-331
Southeast Federal Center
1200 New Jersey Avenue, SE
Washington, DC 20590

If sending from outside of the DOT HQ Buildings, the requestor should use a method of delivery that supports tracking and confirmation of delivery (e.g., FedEx, UPS, or registered mail with confirmation of receipt). The requestor should retain a copy of the Media Sanitization Request Form prior to packaging

the form with the media. The requestor should also send an electronic mail (e-mail) to FHWA ISSM to notify the FHWA ISSM of the shipment.

SANITIZATION OF MEDIA

Upon receipt of the media, the FHWA ISSM will transfer the media to the staff performing the sanitization. Upon completion of the sanitization activity, section III of the form will be completed and sent to the FHWA ISSM for signature. Once signed, the ISSM will send a copy of the completed form to the requestor for their files. The ISSM will also retain a copy.

This Page Intentionally Left Blank

MEDIA SANITIZATION REQUEST FORM

Section I

Requestor Name (Printed):		Date:	
Organization/Office Code:		Phone:	

Upon completion of media sanitization, please handle media as follows:

___ Dispose of Media

___ Return Media to Requestor (specify return address) or Other (please specify):

I certify that any official records within the data contained on the media to be sanitized have been archived in accordance with DOT and NARA directives.

**Authorizing Federal Official Name
and Title (Printed)**

Signature

Section II

Item #	Qty.	Item Control Identifier	Media Type	Request Date	Reason
1.					
2.					
3.					
4.					
5.					

Section III

Media Degaussed By (Name Printed): _____ Signature/Date _____ Verified by (Name Printed): _____ Signature/Date _____

MEDIA SANITIZATION REQUEST FORM

Request Form reviewed by ISSM:

Signature/Date _____

Instructions for Completing Sections I and II

The following table provides the Requester with instructions for completing Section I and Section II of the "Media Sanitization Request Form."

Step #	Instructions
1.	The requestor shall complete Section I with the identifying information. All elements in this section, except the requestor's signature, should be printed clearly and legibly.
2.	One sheet allows up to 5 sanitization requests. Each field should be filled in with clear print. Ditto marks are acceptable if the information in a cell is exactly the same as the information in the cell directly above it.
3.	Qty is the quantity of media, such as 10 hard disks that are being sanitized because they have gone bad, or a sequential series of 20 tapes being sanitized for the same reason.
4.	Item Control Identifier is a unique name or control # - typically this would be present on a label on the media
5.	Media Type is the type of media the requestor needs to have sanitized such as DLT Tape, Hard Drive, Floppy Disk, VHS Tape, etc.
6.	Request Date is the day the requestor fills out the form.
7.	Reason is the reason for sanitizing the media such as bad hard drive, decommissioning system that contained hard drive, tape exceeded usefulness, etc.

**APPENDIX - G FHWA BUSINESS IMPACT
ANALYSIS METHODOLOGY AND
QUESTIONNAIRE**

FHWA Business Impact Analysis (BIA) Methodology

BACKGROUND:

In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, the business impact analysis (BIA) is a key step in the contingency planning process overall. Since FHWA's OITS is in the process of modifying our disaster recovery/ contingency strategy and plans, a BIA needs to be performed. Therefore, information from information system stakeholders, including the information system owners, relating to contingency planning strategies for their respective systems is required. These strategies include accomplishing the following:

- I. **Determining the mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum system downtime that FHWA can tolerate while still maintaining the mission or businesses function.
- II. **Identifying the resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume the system's mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
- III. **Identifying the recovery priorities for system resources.** Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing system recovery activities and resources.

What are the benefits of performing a BIA?

The main benefit of a BIA is to ensure cost-effective measures in respect to information system continuity. Information ascertained via the BIA is aimed at developing a recovery strategy to ensure monies and efforts to recover a system are not overspent. Additionally, for each system, the BIA will provide the following information:

- The criticality of the system relative to the owning organization's mission or business;
- the maximum acceptable length of time that can elapse before unavailability of the system causes an unacceptable impact on the mission/business of the organization;
- the point in time to which the system must be recovered;
- the key resources requirements, computer hardware, software and equipment associated with each major function(s) the system performs; and
- the quantitative and qualitative impacts that will be incurred should a disruption occur.

What is the methodology for performing the BIA?

Initially, the BIA will be performed for all information systems categorized as major applications hosted on the ITD General Support System (GSS). The owners of these systems will be sent an email outlining the purpose and scope of the BIA along with a BIA questionnaire to complete. Subsequently, a meeting will be held with each owner to discuss their questionnaire. This will be a face-to-face meeting to ensure that the system owner understands the purpose and intent of each question on the BIA questionnaire and has provided the correct information for their system. The information provided on each questionnaire will be analyzed and form the basis for completing

the BIA for the ITD GSS. Another outcome of this analysis will be to verify that the current FIPS-199 sensitivity level for availability is correct based on the information provided on the questionnaire.

In the future, the BIA may be expanded to include other FHWA information systems not currently hosted on the ITD GSS.

What is the purpose of the attached FHWA BIA questionnaire?

The FHWA BIA questionnaire is designed to ascertain the pertinent information necessary to identify impact to FHWA's mission or business if an information system is not available and gauge the impact over various time periods of unavailability of the system.

Attached below is the BIA Questionnaire designed to identify impact to FHWA's mission.



Business Impact
Analysis Questionnaire