Telematics Cybersecurity Primer for Agencies

Prepared for:

The Department of Homeland Security
Science and Technology Directorate
Cyber Security Division
Washington, DC 20528

Prepared by:
Jack Clark, Daniel Chin
Advanced Vehicle Technology Division, V337
Volpe National Transportation Systems Center
U.S. Department of Transportation

June 27, 2017

Table of Contents

List of Acronyms

C&A – Certification and Authorization
CDMA – Code Division Multiple Access
CIA – Confidentiality, Integrity, Availability
CVE – Common Vulnerabilities and Exposures
DHS – Department of Homeland Security
DOS – Denial of Service
ECU – Electronic Control Unit
EO – Executive Order
FIPS – Federal Information Processing Standards
FIRST – Forum of incident Response and Security Teams
FISMA – Federal Information Security Management Act
FMIS – Fleet Management Information System
GSM – Global System for Mobile communication
NFC – Near-Field Communication
NIST – National Institute of Standards and Technologies
NTIA - National Telecommunications and Information Administration
IA – Information Assurance
IEC – International Electrotechnical Commission
IoT – Internet of Things
IP – Internet Protocol
IS – Information System
ISO – International Organization for Standardization
IT – Information Technology
RMF – Risk Management Framework
SOTA – Secure Over-The-Air Update
SP – Special Publication
TLS – Transport Layer Security
TUF – The Update Framework

Executive Summary

Executive Order (EO) 13693, “Planning for Federal Sustainability in the Next Decade”, states that government agencies are responsible for:

“…collecting and utilizing as a fleet efficiency management tool…agency fleet operational data through deployment of vehicle telematics at a vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate”

The goal of this document is to provide government agencies responsible for the selection and procurement of a fleet efficiency management tool, herein referred to as Fleet Management Information System (FMIS) with situational awareness of potential cybersecurity risks surrounding the implementation of such a tool. Additionally, security professionals and government cybersecurity officials can use this document as a security baseline when performing cybersecurity assessments on products deployed on government vehicles. This document is directed towards government agencies responsible for the selection and procurement of a FMIS, and is in no way meant to dissuade an agency from striving for compliance with the EO or to persuade management to seek relief from implementation of the EO. The intent of the document is to raise awareness of the responsibility for managing risk related to cybersecurity when selecting and implementing a FMIS within an agency.

Central to a FMIS is the retrieval, transmission, assessment, and storage of vehicle data. When data is collected, transmitted and/or stored by a government agency, the processes and systems involved in these actions fall under the Federal Information Security Management Act (FISMA). To that end, the main body of the document centers on the requirements of FISMA and draws on guidance found within the National Institute of Standards and Technologies (NIST) Special Publications (SP). It is recommended that those not familiar with either the requirements of FISMA or their agencies policies and procedures for implementing FISMA, consultation with agency staff responsible for Information Security (IS) and/or Information Assurance (IA) at the enterprise level is recommended.

This document addresses the core concerns for an agency in the protection of their fleet management data, systems, and assets. This protection includes communications to and from the vehicle, vehicle systems, and government data being transmitted and stored. Implementing this protection involves:

- Protecting communications within the tool via the use of encryption, authentication, etc.
- Protecting the tool itself via software and firmware protection through the use of digital signatures, encryption, etc.
- Protecting actions of the tools via the use of minimal rights and enabling of minimal services, etc.
- Protecting the integrity of the tool via authentication, vulnerability management, penetration testing, etc.

Ensuring the security posture of an agencies information technology systems should always remain a high priority. To meet this goal, government agencies must be especially diligent in ensuring the IA posture of all systems inherent in, or incorporated into vehicles, products, and services that are part of the FMIS.

1.0 Background

The goal of this document is to provide government agencies responsible for the selection and procurement of a FMIS with situational awareness of potential cybersecurity risks surrounding the implementation of such a tool. Additionally, security professionals and government cybersecurity officials can use this document as a security baseline when performing cybersecurity assessments on products deployed on government vehicles.

As agencies initiate actions for compliance with EO 13693, "Planning for Federal Sustainability in the Next Decade"[1] dated June 10, 2015, government agencies will be looking to vehicle manufacturers and third-party vendors for solutions to assist them in meeting the mandate of integrating vehicle telematics. This document is intended to:

1. Provide a primer for agencies to help them in understanding the security risk(s) associated with integration of vehicle telematics.
2. Foster situational awareness for agencies regarding their responsibility for managing risk to their assets, data, and personnel.

When planning for a FMIS, it is essential to understand that in addition to the incorporation of telematics[2] within the vehicle, as directed by EO 13693, implementation of a tool will also introduce a new IS within the enterprise. As with all enterprise level IS solutions, the IS owner, in this case the agency, bears the responsibility not just for the operational efficiency and cost effectiveness of the solution but also for managing the security and protection of both the IS and the data being collected, managed, and stored. This responsibility is detailed in the Federal Information Security Management Act of 2014[3]. Figure 1 illustrates a high-level generalization of the significant components associated with a complete FMIS.

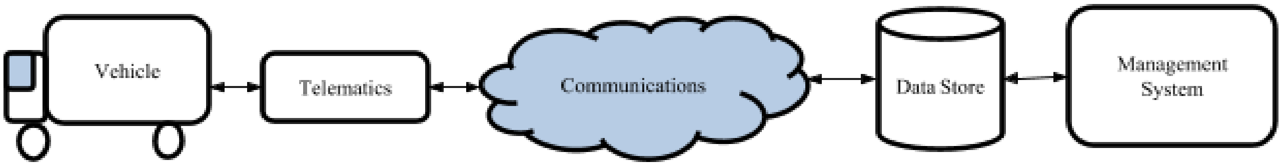


Figure 1. Components of a Fleet Management Information System (FMIS)

The complete FMIS includes at a minimum the vehicle, some form of telematics, a

[1] **E.O. 13693 section 3(g) (iii):** *collecting and utilizing as a fleet efficiency management tool, as soon as practicable but not later than two years after the date of this order, agency fleet operational data through deployment of vehicle telematics at a vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate.*

[2] **Telematics** *is a combination of the words telecommunications and informatics. Telematics, in a broad sense, is any integrated use of telecommunications with information and communications technology. It is the technology of sending, receiving and storing information relating to remote objects – like vehicles – via telecommunication devices.*

[3] **Reference:** *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*

communications infrastructure, a management system, and a database. The management system and data store components are commonly referred to as the '"back-end" system'. Throughout this document, references will be made to 'fleet management system', 'telematics', and '"back-end" system'. For reference, all discussion points or examples within the document are applicable to all components of the FMIS, which includes all components from the vehicle to the database as depicted in Figure 1. There are times when the implementation of controls at a specific component level (i.e. telematics, back-end system, etc.) is of significant importance and will be called out as necessary. For this document, the significance of each component to the security of the FMIS is based on the role of the component and/or other systems' reliance on that component. These roles and reliance are briefly described below:

- **Vehicle** – The vehicle component of the FMIS is responsible for producing the data that drives the requirement for fleet management. The vehicle is an especially challenging component regarding cybersecurity. The following areas contribute to the challenges of cybersecurity in the vehicle:
    1) Data is communicated via a network inherent to the vehicle;
    2) The vehicle network is proprietary to the vehicle manufacturer;
    3) Vehicle networks are designed for performance at the cost of security;
    4) Many vehicles allow vehicle performance and safety systems to reside on the same network; and
    5) Some vehicle networks have been proven to be vulnerable to unauthorized access from remote sources.
- **Telematics** –The telematics component of the FMIS is arguably the most important component for security control review and implementation. The telematics device becomes a gateway between the vehicle and the communications infrastructure required for transmitting vehicle data to a back-end system. As previously noted, vehicle networks present vulnerabilities since they are designed for performance at the cost of security. Once incorporated into the vehicle, the telematics device provides the gateway to this vulnerable network. In this environment, the security of the telematics device is paramount to the security of the vehicle.
- **Communications** – The communications component of the FMIS encompasses wireless, directly connected, Near-Field Communications (NFC), and Internet Protocol (IP) communications. These communications vary between serial cable connectivity for device diagnostics to mobile communications such as Global System for Mobile (GSM) communication, Code Division Multiple Access (CDMA), etc. Regardless of the communication method, each one extends and essentially provides access to the telematics device that, in turn, provides access to the vehicle network.
- **Management System** – The management system component of the FMIS is comprised of a user interface, processing devices, and methods required for presenting the vehicle data to an agency in a useable format. These components commonly include publicly-connected Internet web servers and vendor controlled and managed back-end servers. The management system is essentially the gateway to the vehicle data. The agency should be aware of the policies, controls, and protections in place for protecting access to these systems.
- **Data Store** – The database component of the FMIS is another significant area for security control review and implementation, possibly more specific on the policy and legal side for vendor controlled data stores. Focus on this area cannot be overstated;

this area of the FMIS is where all the logistical data for a fleet is correlated and stored. It is vital for an agency to be fully aware of how this data is processed, accessed, managed, stored, and controlled specially on a vendor system/facility.

As agencies explore options for designing, procuring, or enhancing a FMIS to meet the requirements of EO 13693, there is a high probability to include either a complete vendor solution, or multiple vendor solutions for individual components of the tool. When evaluating possible solutions, agencies should ensure that a comprehensive approach to IA is a contributing factor in the selection of a FMIS or any enhancements to an existing FMIS. Ensuring that IA is a consideration in the design or procurement of the tool is not only a responsible approach, it is also mandated by the enacting of the National Institute of Standards and Technology (NIST) Federal Information Security Management Act (FISMA). In accordance with FISMA, agencies must adhere to a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. When selecting a FMIS, it is the responsibility of the fleet management office, as the system owner, to ensure the system maintains compliance with FISMA guidance throughout the system lifecycle.

2.0 Fleet Management Office Responsibility- FISMA and FIPS 199

The fleet management office, as the procurer and maintainer of the FMIS, assumes the role of the “system owner”. As a system owner, the fleet management office is responsible for compliance with FISMA, which defines a framework for managing information security. FISMA must be followed for all information systems used or operated by both federal and state government agencies, including all information systems in the executive or legislative branches, or by a contractor or other organization on behalf of an agency. In accordance with FISMA, NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing information security which are usable by all federal and state agencies. FISMA requires the system owner to implement security controls, policies, and guidance to ensure an agency’s systems remain secure and monitored throughout the system lifecycle. FISMA also requires each agency to incorporate a Certification and Authorization (C&A) process to ensure oversight of FISMA compliance. Although FISMA does not direct a specific implementation of the C&A process, it is common for a single authorizing office within an agency to take responsibility for authorizing information systems prior to them being allowed to operate within the agency. It is the responsibility of the fleet management office to coordinate authorization activities with the appropriate officials within their agency.

2.1 Federal Information Processing Standard (FIPS) 199

The following guidance is pertinent to Federal and State agencies who are procuring or implementing a Fleet Management Information System (FMIS) and is the first step in assessing cybersecurity risks for FMIS’s is defining the System Categorization level of your FMIS:

The FIPS Publication Series from the National Institute of Standards and Technology (NIST) are the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology

Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the federal government.

FIPS Publication 199-*Standards for Security Categorization of Federal Information and Information Systems* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf addresses the categorizing of information and information systems as either Low, Medium or High and *NIST Special Publication 800-53* provides guidance on recommended security controls based on the system categorization level and impacts, https://nvd.nist.gov/800-53.

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes:

(i) Effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities

(ii) Consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices

Security Objectives

FISMA defines three security *objectives* for information and information systems:

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is **LOW** if—

‒ The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
(ii) Result in minor damage to organizational assets
(iii) Result in minor financial loss
(iv) Result in minor harm to individuals

The *potential impact* is **MODERATE** if—

‒ The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
(ii) Result in significant damage to organizational assets
(iii) Result in significant financial loss
(iv) Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries

The *potential impact* is **HIGH** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions

(ii) Result in major damage to organizational assets

(iii) Result in major financial loss

(iv) Result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

3.0 Cybersecurity Guidance Background

IA is the practice of managing risks to information and information systems. The main tenets of IA are to ensure the security triad of confidentiality, integrity, and availability (commonly referred to as CIA). Significant methods of providing IA include the prevention, detection, and response to attacks against a system and/or information processed by a system. As referred to by the Department of Homeland Security (DHS), this prevention, detection, and response to attacks are the main components of cybersecurity.

A comprehensive approach to implementing cybersecurity controls should be viewed as a significant contributing factor when selecting any FMIS. Many resources exist to aid agencies in their evaluation of technologies, products, and information systems, many of which are referenced in Appendix A.

For the examples supplied within this document, the SP series developed by NIST will be referenced. More specifically, this document will use the NIST SP 800-53 Rev 4, entitled *"Security and Privacy Controls for Federal Information Systems and Organizations*", to illustrate some of the security controls within the guidance which have a high probability of being essential controls applicable to a FMIS.

NIST SP 800-53 Rev 4 was developed to guide agencies as they implement security measures to protect government information, operations, and assets. The abstract of NIST SP 800-53 Rev 4, NIST describes the publication as:

> "…*a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors"*.

This catalog of security and privacy controls addresses security from both a functionality perspective and an assurance perspective. Functionality refers to the strength of security functions and mechanisms provided, and security assurance refers to the measures of confidence in the implemented security capability. Addressing security, functionality, and IA ensures that Information Technology (IT) components and the information systems built from those components use strong systems and security engineering principles, which make the systems sufficiently trustworthy.

There are many contributing factors and intricacies in applying a system security framework such as NIST SP 800-53 Rev 4 to an information system. Therefore, this document is not inclusive of FISMA and system security requirements, and is not intended to be a comprehensive guide to assessing and implementing security. The anticipated audience of this document is those individuals involved in the procurement of a FMIS who may not have a security background or awareness of federal requirements for implementing a secure system baseline.

4.0 Security Controls

This document follows the framework of the NIST SP 800-53 security controls. These security controls have a well-defined structure organized into eighteen control families. Each family contains a set of security controls related to the general security topic of the control family. Each control involves aspects of policy, oversight, supervision, manual processes, actions by individuals, and/or automated mechanisms recommended for implementation in the information system (technical) or by the owner of the information system (policy, procedure, etc.). Table 1 identifies the eighteen security control families defined in NIST SP 800-53 Rev 4.

Table 1. NIST SP 800-53 Rev 4 Security Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	**MP**	Media Protection
AT	Awareness and Training	**PE**	Physical and Environmental Protection
AU	Audit and Accountability	**PL**	Planning
CA	Security Assessment and Authorization	**PS**	Personnel Security
CM	Configuration Management	**RA**	Risk Assessment
CP	Contingency Planning	**SA**	System and Service Acquisition
IA	Identification and Authentication	**SC**	System and Communications Protection
IR	Incidence Response	**SI**	System and Information Integrity
MA	Maintenance	**PM**	Program Management

NIST SP 800-43 Rev 4 contains 16 program management and 240 individual security controls[4].

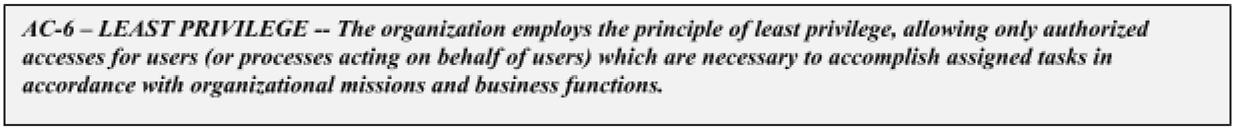
[4] **Security Controls** – *This count does not include the privacy controls included in NIST SP 800-53 Rev 4.*

Subsets of controls are applicable to a system depending on the security categorization of the system. The security categorization is based on the potential impact to an organization should an event occur to jeopardize the information or information system[5]. There are three levels of potential impact, defined as LOW (L), MODERATE (M), or HIGH (H). In regards to applicable controls per categorization, there are 170 applicable controls defined for a HIGH categorization, 159 applicable controls defined for a MODERATE categorization, and 115 applicable controls for a LOW categorization.

The following subsections describe a small subset of controls from within the NIST 800-53 Rev 4 control families. The controls chosen were selected based on their applicability in addressing common shortcomings and/or vulnerabilities identified through assessments of current FMIS offerings.

[5] **System Categorization** – *Details on categorizing a system can be found within NIST documents and more specifically in the Federal Information Processing Standard 199 (FIPS-199). The process of categorizing a system are outside of the scope of this guidance.*

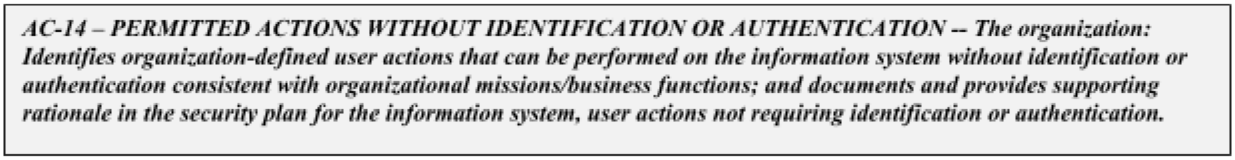
4.1 Access Control



AC-6 – LEAST PRIVILEGE -- The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

While some components of a FMIS will support authentication, i.e., username/password pairs, digital signatures, etc., it is unlikely all components will support authentication. For example, implementing authentication for telematics units within the vehicle may void the vehicle warranty or introduce an unintended denial of service if there is a malfunction in the authentication system. Agencies should ensure all actions taken by the FMIS that are capable of supporting some form of authentication are configured so that the minimal privilege required to perform an action is provisioned to a user's account.

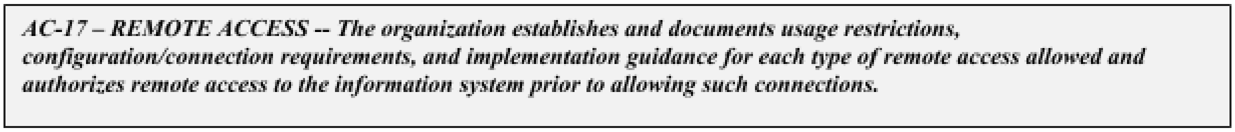
For further information refer to NIST SP 800-53 Rev 4 Control AC-6 supplemental guidance section.



AC-14 – PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION -- The organization: Identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

It is likely that execution of system/user actions such as communications between the telematics unit and the vehicle, or telematics unit and the communications infrastructure will not be capable of implementing controls associated with user authentication. Agencies should require that vendors provide documentation that justifies the need for a FMIS to perform actions that cannot support enforcement of access, authentication and/or execute with elevated privileges.

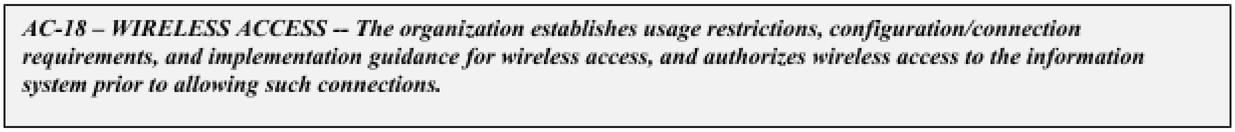
For further information refer to NIST SP 800-53 Rev 4 Control AC-14 supplemental guidance section.



AC-17 – REMOTE ACCESS -- The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorizes remote access to the information system prior to allowing such connections.

For the process of communicating with the vehicle or accessing the components of a back-end system, remote access to one or more components is a fundamental feature of the FMIS in meeting the mission need. Agencies should require that vendors document all remote access allowed to, or required by, all components of the FMIS. Agencies should work with the vendor to ensure safeguards are implemented to protect access to and storage of government data.

For further information refer to NIST SP 800-53 Rev 4 Control AC-17 supplemental guidance, NIST SP 800-46, NIST SP 800-77, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121.

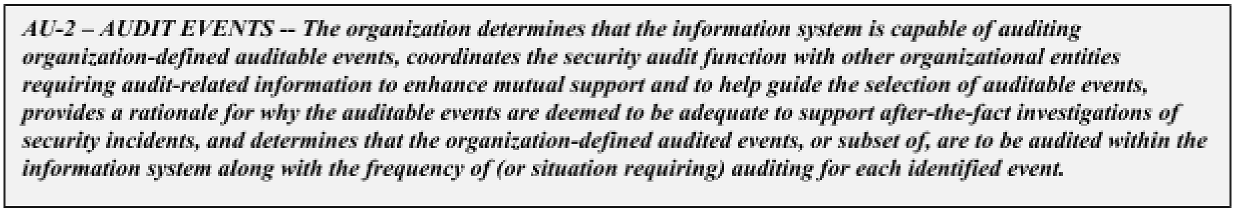


AC-18 – WIRELESS ACCESS -- The organization establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access, and authorizes wireless access to the information system prior to allowing such connections.

Wireless access points may be present at multiple points within the FMIS, including built-in to the vehicle or telematics system. Examples of wireless communications within a vehicle may include technologies such as Bluetooth or satellite communications for the infotainment system or telematics unit, Wi-Fi communications present as a hotspot or means of connecting to a remote network, infrared communications and Radio Frequency Identification (RFID) for vehicle automation, etc. The presence and use of each of the previously referenced technologies need to be reviewed for implementation of security controls. Agencies should ensure they are aware of all methods of wireless access available throughout the FMIS.

For further information refer to NIST SP 800-53 Rev 4 Control AC-18 supplemental guidance, NIST SP 800-48, NIST SP 800-94, NIST SP 800-97.

4.2 Audit and Accountability

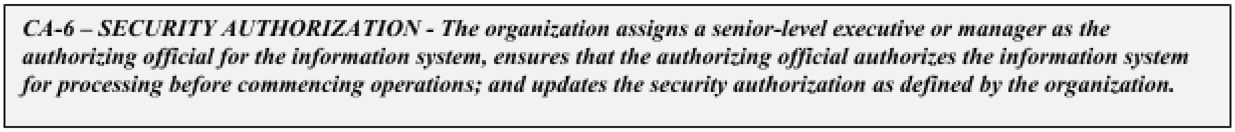


AU-2 – AUDIT EVENTS -- The organization determines that the information system is capable of auditing organization-defined auditable events, coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events, provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents, and determines that the organization-defined audited events, or subset of, are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.

Auditing of events and producing system logs are critical to ensuring both proper operations and security of a system. If a system is not capable of or configured to produce information related to system operations, it is impossible to be either reactive or proactive in the maintenance or securing of the system. Agencies should ensure that all components of the FMIS are capable of auditing events the agency deems necessary to ensure the system is operated in a secure and safe manner.

For further information refer to NIST SP 800-53 Rev 4 Control AU-2 supplemental guidance, NIST SP 800-92, www.idmanagement.gov.

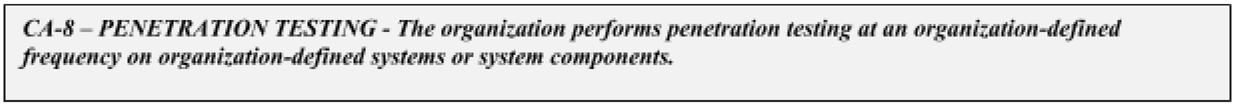
4.3 Security Assessment and Authorization



CA-6 – SECURITY AUTHORIZATION - The organization assigns a senior-level executive or manager as the authorizing official for the information system, ensures that the authorizing official authorizes the information system for processing before commencing operations; and updates the security authorization as defined by the organization.

Agencies should coordinate with their Chief Information Officer and/or system authorization branch to determine any agency specific requirements for authorizing the fleet management system/solution within the agency. Agencies should initiate discussion with the authorization branch prior to procuring a fleet management system. Understanding authorization needs prior to procurement of a telematics system will help to ensure that the necessary vendor information, such as system interconnections, continuous monitoring of system, incidence response activities, vulnerability management, etc., is requested from the vendor and made available to the agency.

For further information refer to NIST SP 800-53 Rev 4 Control CA-6 supplemental guidance, OMB Circular A-130, OMB Memorandum 11-33, NIST SP 800-37, NIST SP 800-137.

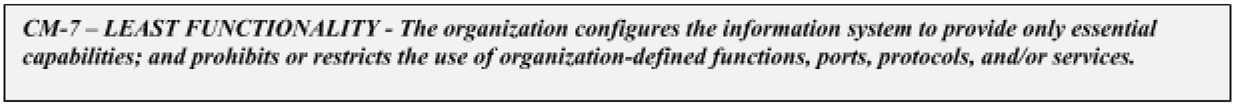


CA-8 – PENETRATION TESTING - The organization performs penetration testing at an organization-defined frequency on organization-defined systems or system components.

In a system with diverse technologies such as a FMIS and associated services, different components are likely to be produced by different vendors. For example, a fleet management service provider may provide the back-end system, but procure the telematics devices and/or communications infrastructure from another vendor. The agency must be aware of the security posture of all of these disparate services and/or components. The most reliable method of ensuring awareness of system vulnerabilities and cross checking against vendor supplied documentation regarding the security posture of a system/component is to have a third-party, i.e. an entity not beholden to the agency or vendor, perform an independent penetration and/or security assessment. Penetration testing is a process used to attempt to evaluate the security of a system/component by safely identifying and exploiting vulnerabilities. Agencies should ensure that all applicable components of the FMIS undergo a third-party, independent penetration test, and that the agency is provided acceptable insight to the results of the testing.

For further information refer to NIST SP 800-53 Rev 4 Control CA-8 supplemental guidance.

4.4 Configuration Management

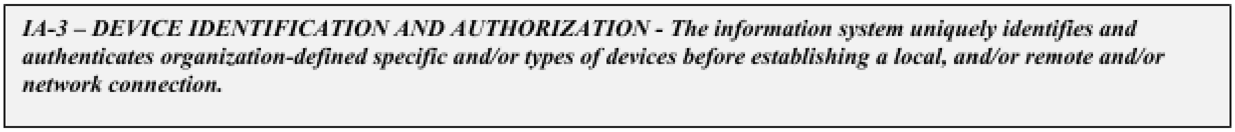


CM-7 – LEAST FUNCTIONALITY - The organization configures the information system to provide only essential capabilities; and prohibits or restricts the use of organization-defined functions, ports, protocols, and/or services.

Multiple vendors may be involved in the configuration of a fleet management system/solution. Frequently, a vendor or provider of the component or service will include a means to access the device for diagnostics and maintenance. Oftentimes the vendor providing the fleet management solution/service is not aware of the configuration or access methods of procured components within their system, i.e. telematics and communications. Agencies should ensure that they are aware of all the interrelation of all components within the FMIS, and that these components have been configured to only use services necessary for secure operations of the system. Examples of unnecessary services include: File Transfer Protocol, telnet, Short Messaging Service, etc. Agencies should ensure that any services used for testing or troubleshooting are disabled or properly protected from unauthorized access and use.

For further information refer to NIST SP 800-53 Rev 4 Control CM-7 supplemental guidance, DoD Instruction 8551.01.

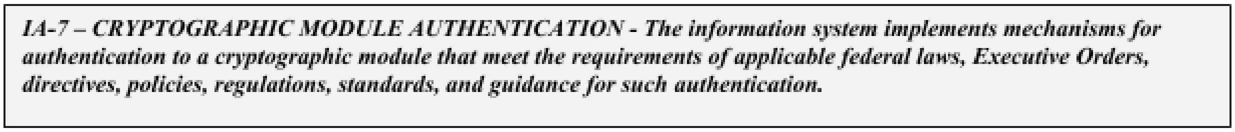
4.5 Identification and Authentication



IA-3 – DEVICE IDENTIFICATION AND AUTHORIZATION - The information system uniquely identifies and authenticates organization-defined specific and/or types of devices before establishing a local, and/or remote and/or network connection.

A FMIS will consist of communications between various types of components such as from the telematics device to the communications network, the back-end system to the communications network, and the telematics device to the back-end system. Agencies should ensure all components of the FMIS are configured to uniquely authenticate components of the system and or any other interfacing system such as agency financial systems, monitoring systems, etc. Where unique authentication inhibits functionality an agency should request documented justification for the absence of the security control along with mitigating controls in place to reduce risk associated with not implementing the security control.

For further information refer to NIST SP 800-53 Rev 4 Control IA-3 supplemental guidance.

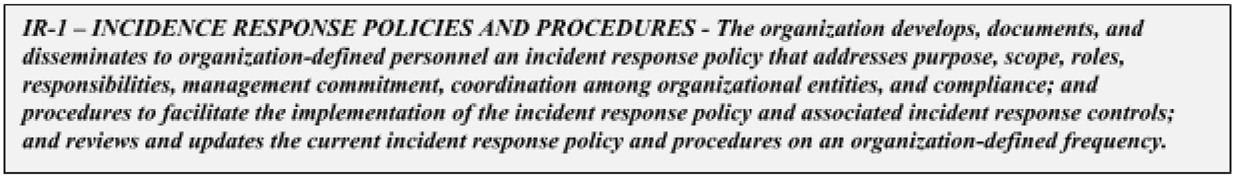


IA-7 – CRYPTOGRAPHIC MODULE AUTHENTICATION - The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Where devices cannot support user interaction a secure baseline may include the use of encryption and digital certificates. If the FMIS makes use of encryption for any processes, agencies should ensure that the use of supporting cryptographic modules is compliant with government requirements detailed within the Federal Information Processing Standards 140-2 and recommendations found in the NIST SP series.

For further information refer to NIST SP 800-53 Rev 4 Control IA-7 supplemental guidance, FIPS Publication 140-2, NIST SP 800-175B, csrc.nist.gov/groups/STM/cmvp/index.html.

4.6 Incidence Response



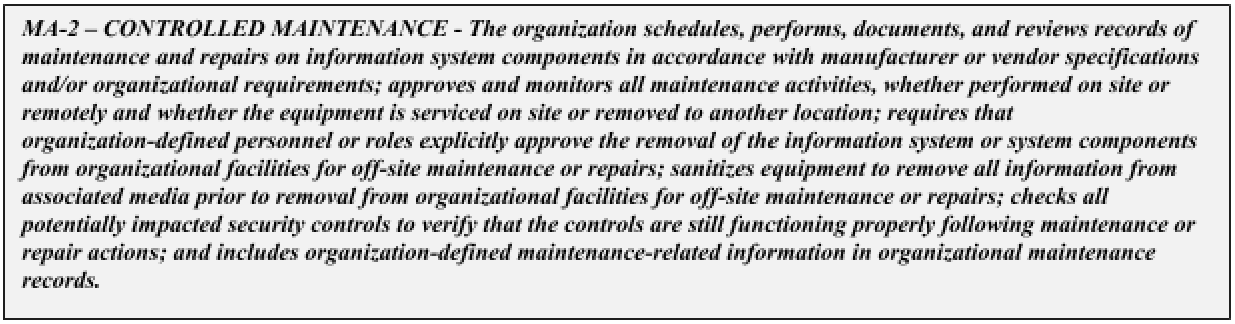
IR-1 – INCIDENCE RESPONSE POLICIES AND PROCEDURES - The organization develops, documents, and disseminates to organization-defined personnel an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the incident response policy and associated incident response controls; and reviews and updates the current incident response policy and procedures on an organization-defined frequency.

Agencies are responsible for developing plans and procedures for identifying and responding to incidents occurring due to events such as security breaches, misuse, malicious activity, system outages, etc. Proactive maintenance of the system baseline and security posture is one of the core components of incident management. As multiple vendors may be involved in the configuration of a FMIS, open lines of communication and sharing of information related to security incidents between an agency and system/component vendors is key to proper implementation of this control.

For further information refer to NIST SP 800-53 Rev 4 Control IR-1 supplemental guidance, NIST

SP 800-12, NIST SP 800-61, NIST SP 800-83, NIST SP 800-100.

4.7 Maintenance

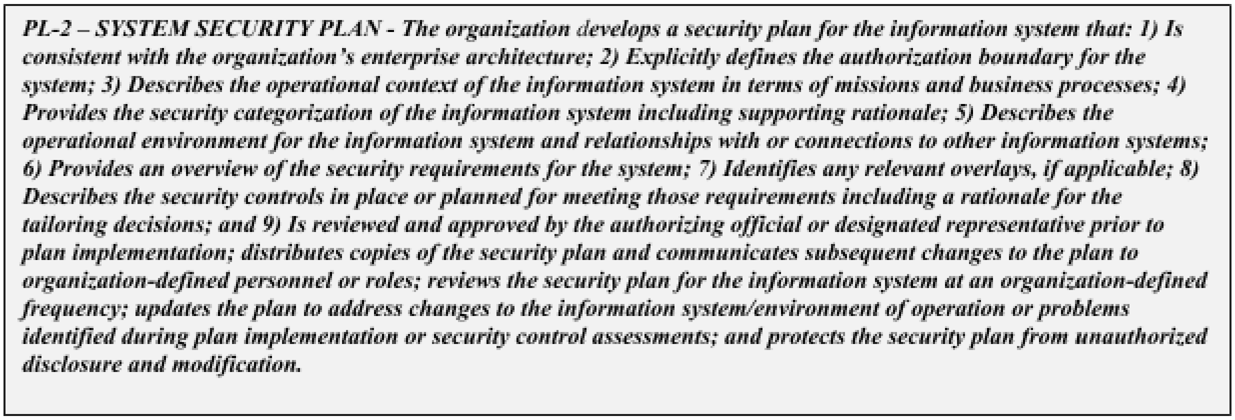


MA-2 – CONTROLLED MAINTENANCE - The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and includes organization-defined maintenance-related information in organizational maintenance records.

Agencies should ensure that policies and procedures exist to control maintenance of FMIS components such as updating of telematics devices, performing maintenance or modifications of devices, etc. Agencies should ensure that components outside of their direct control are not updated or modified without prior coordination and approval by an organization defined individual or role. Agencies should ensure that any component of the FMIS is sanitized of any and all government data prior to dispositioning or disposal of the component.

For further information refer to NIST SP 800-53 Rev 4 Control MA-2 supplemental guidance.

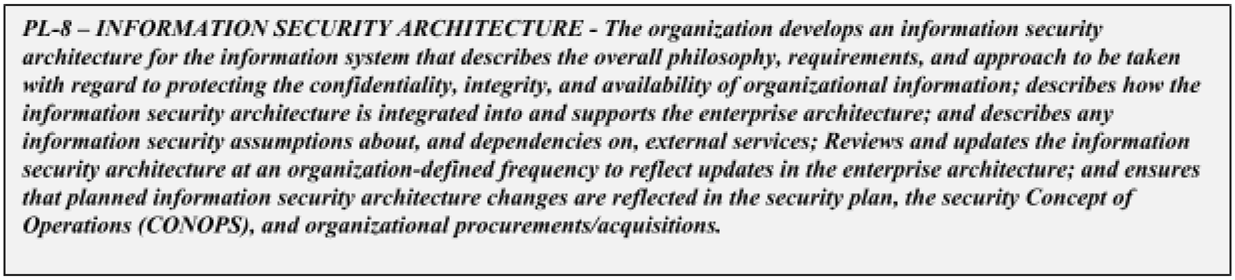
4.8 Planning



PL-2 – SYSTEM SECURITY PLAN - The organization 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; distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles; reviews the security plan for the information system at an organization-defined frequency; updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and protects the security plan from unauthorized disclosure and modification.

Agencies should ensure that there is a clear and concise understanding of the authorization boundary of the FMIS; i.e., which entity has responsibility for each component of the system. Agencies should ensure that their organization has full knowledge of the system baseline and security posture within their boundary and that they can detail compliance of the system to all applicable security controls required for implementation by government standards. It is recommended that an agency implement a vulnerability scanning and assessment process in maintaining a stable and secure information security architecture.

For further information refer to NIST SP 800-53 Rev 4 Control PL-2 supplemental guidance, NIST SP 800-18.

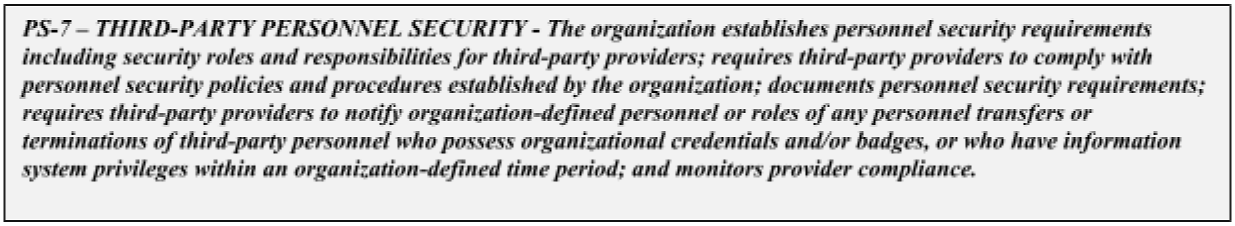


PL-8 – INFORMATION SECURITY ARCHITECTURE - The organization develops an information security architecture for the information system that describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; describes how the information security architecture is integrated into and supports the enterprise architecture; and describes any information security assumptions about, and dependencies on, external services; Reviews and updates the information security architecture at an organization-defined frequency to reflect updates in the enterprise architecture; and ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

As multiple vendors may be involved in the FMIS, agencies should ensure they have insight into each vendor's approach to information security. Knowledge of the vendor's focus on information security, for example compliance with industry best practices, etc., will provide information necessary for properly evaluating the risk of having government data collected, managed, and stored by a third-party organization.

For further information refer to NIST SP 800-53 Rev 4 Control PS-8 supplemental guidance, NIST SP 800-35.

4.9 Personnel Security

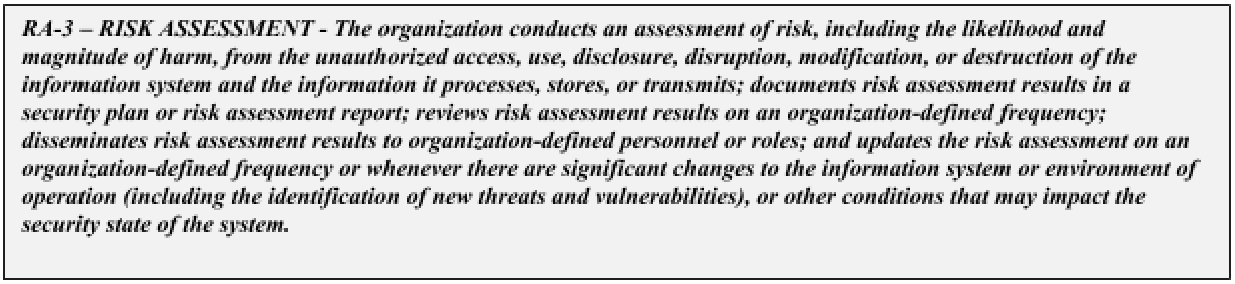


PS-7 – THIRD-PARTY PERSONNEL SECURITY - The organization establishes personnel security requirements including security roles and responsibilities for third-party providers; requires third-party providers to comply with personnel security policies and procedures established by the organization; documents personnel security requirements; requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization-defined time period; and monitors provider compliance.

Agencies procuring a FMIS as a service should ensure they understand the security policies and human resource concept of the service provider. Any insight into the service providers hiring practices, corporate culture, attrition rate, etc., will provide information that can aid in evaluating the risk of having government data collected, managed, and stored by a third-party organization.

For further information refer to NIST SP 800-53 Rev 4 Control PS-7 supplemental guidance, NIST SP 800-35.

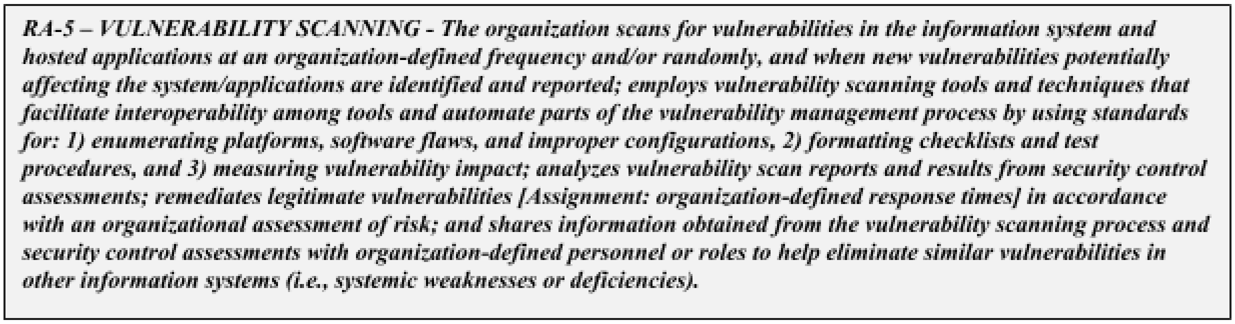
4.10 Risk Assessment



RA-3 – RISK ASSESSMENT - The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; documents risk assessment results in a security plan or risk assessment report; reviews risk assessment results on an organization-defined frequency; disseminates risk assessment results to organization-defined personnel or roles; and updates the risk assessment on an organization-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Agencies should ensure a risk assessment is conducted relative to implementing a FMIS within the agency, as well as a risk assessment of the FMIS itself. Risk management is the evaluation of the business risk associated with the use, ownership, operation, involvement, influence and adoption of information technology within an enterprise or organization. Generally speaking, risk is the product of likelihood of a security event and the impact of that event. The measure of risk can be determined as a product of threat, vulnerability and asset value. The risk assessment should pay specific attention to any system components not under direct control of the agency. These components could be a significant area of concern if they are involved in the collecting and storing of agency logistical data, specifically vehicle locations, patterns of use, Personally Identifiable Information (PII), etc.

For further information refer to NIST SP 800-53 Rev 4 Control RA-3 supplemental guidance, OMB Memorandum 04-04, NIST SP 800-30, NIST SP 800-39, www.idmanagement.gov.

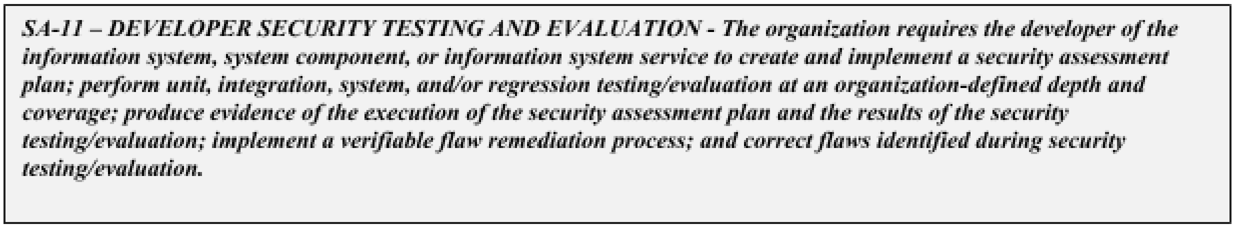


RA-5 – VULNERABILITY SCANNING - The organization scans for vulnerabilities in the information system and hosted applications at an organization-defined frequency and/or randomly, and when new vulnerabilities potentially affecting the system/applications are identified and reported; employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1) enumerating platforms, software flaws, and improper configurations, 2) formatting checklists and test procedures, and 3) measuring vulnerability impact; analyzes vulnerability scan reports and results from security control assessments; remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and shares information obtained from the vulnerability scanning process and security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

As multiple vendors may be involved in the FMIS, agencies should ensure that vendors provide clear and concise vulnerability management and incident response plans for system/components and services under their management or control. These plans should address methods of receiving notification of discovered vulnerabilities in their components and the processes in place and or planned for mitigating these vulnerabilities.

For further information refer to NIST SP 800-53 Rev 4 Control RA-5 supplemental guidance, NIST SP 800-40, NIST SP 800-70, NIST SP 800-115, cwe.mitre.org, nvd.nist.org, ISO/IEC 29147.

4.11 System and Service Acquisition

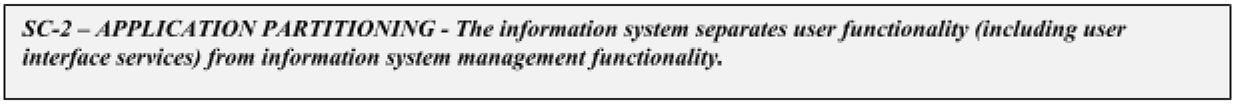


SA-11 – DEVELOPER SECURITY TESTING AND EVALUATION - The organization requires the developer of the information system, system component, or information system service to create and implement a security assessment plan; perform unit, integration, system, and/or regression testing/evaluation at an organization-defined depth and coverage; produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.

Agencies should require vendors to provide documentation of third-party security testing and evaluation of their system and/or components. The documentation should include all results of the security testing and evaluation, including discovered vulnerabilities and a plan/process to mitigate the discovered vulnerabilities or weaknesses in the system. Agencies should ensure they have acceptable access to this documentation and that any redacted sections, such as those that detail vulnerabilities not yet mitigated, are properly justified.

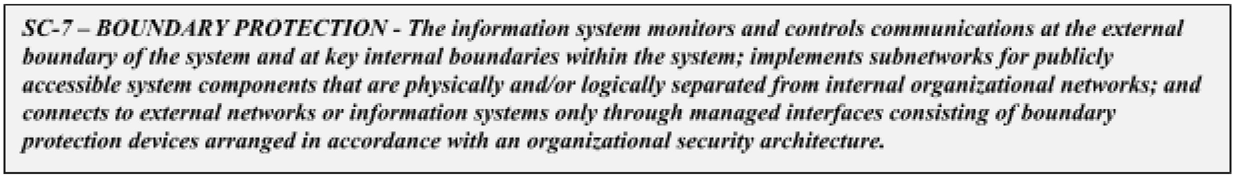
For further information refer to NIST SP 800-53 Rev 4 Control SA-11 supplemental guidance, NIST SP 800-53A, ISO/IEC 15408, cwe.mitre.org, nvd.nist.gov, capec.mitre.org.

4.12 System and Communication Protocols


SC-2 – APPLICATION PARTITIONING - The information system separates user functionality (including user interface services) from information system management functionality.

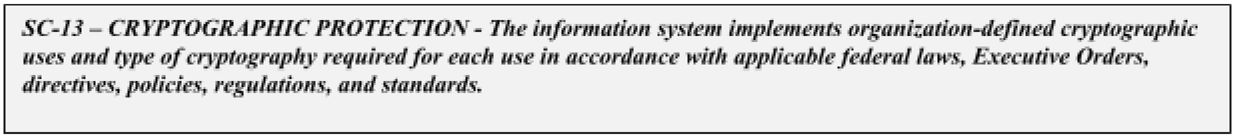
Agencies should ensure that the FMIS is designed in a manner that separates basic user functions from system or privileged level functions. Agencies should be aware of the design and/or management of devices connected directly to the vehicle network and ensure the vehicle is protected against malicious traffic or Denial of Service (DOS) attacks being sent to the vehicle.

For further information refer to NIST SP 800-53 Rev 4 Control SC-2 supplemental guidance.


SC-7 – BOUNDARY PROTECTION - The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

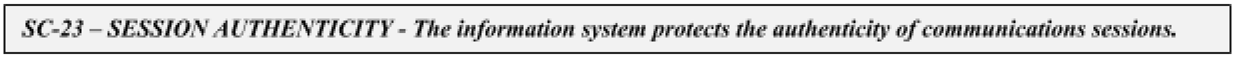
Agencies should ensure that the FMIS provides agency acceptable monitoring and/or protection at appropriate or component boundaries. Agencies should ensure that monitoring and alerting controls and/or processes are in place for notification of unauthorized attempts to access components of the FMIS.

For further information refer to NIST SP 800-53 Rev 4 Control SC-7 supplemental guidance, FIPS Publication 199, NIST SP 800-41, NIST SP 800-77.


SC-13 – CRYPTOGRAPHIC PROTECTION - The information system implements 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.

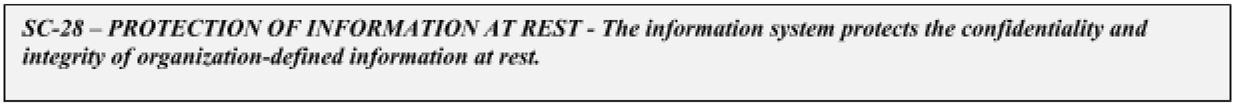
Agencies should ensure that any cryptographic technologies used are configured in compliance with government requirements and/or best practices. These requirements are detailed in the FIPS documentation, and further guidance for use of cryptographic technologies and practices such as digital certificates, use of unique keys, key exchange, key management, etc., can be found in the NIST SP series.

For further information refer to NIST SP 800-53 Rev 4 Control SC-13 supplemental guidance, FIPS Publication 140, csrc.nist.gov/cryptval, cnss.gov.


SC-23 – SESSION AUTHENTICITY - The information system protects the authenticity of communications sessions.

Forms of communications for FMIS s include, at a minimum, data sent between the vehicle telematics devices and the back-end system via cellular communications, communications used for management functions such as website access, and communications between management systems and data stores. Agencies should ensure that communications sessions are properly protected to guard against attacks such as session hijacking, data sniffing, and traffic manipulation.

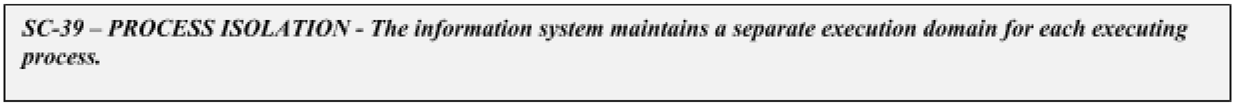
For further information refer to NIST SP 800-53 Rev 4 Control SC-13 supplemental guidance, NIST SP 800-52, NIST SP 800-77, NIST SP 800-95.



SC-28 – PROTECTION OF INFORMATION AT REST - The information system protects the confidentiality and integrity of organization-defined information at rest.

The agency should categorically define any data considered not releasable to the public due to its sensitivity, and develop requirements for protection of that data at rest, i.e. while stored on a telematics devices, management system, or data store. It is the responsibility of an agency designated individual to categorize the content of all data gathered and processed by the FMIS.

For further information refer to NIST SP 800-53 Rev 4 Control SC-28 supplemental guidance, NIST SP 800-56, NIST SP 800-57, NIST SP 800-111.

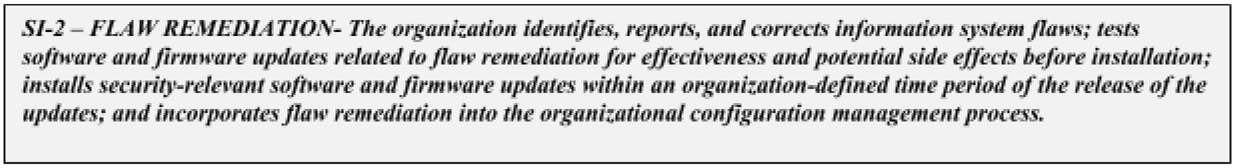


SC-39 – PROCESS ISOLATION - The information system maintains a separate execution domain for each executing process.

Agencies should ensure that the FMIS implements a means to separate execution domains and/or processes. Special attention should be given to research process isolation within both the telematics device and back-end system. Any telematics devices that interfaces directly to the vehicle network should maintain minimum interfacing between the serial communications in the telematics device and the interface to the vehicle network. In assessing the back-end system Agencies should ensure they are informed of all parties using or accessing the back-end system, i.e. a vendor's customer base, foreign government agencies, etc.

For further information refer to NIST SP 800-53 Rev 4 Control SC-39 supplemental guidance.

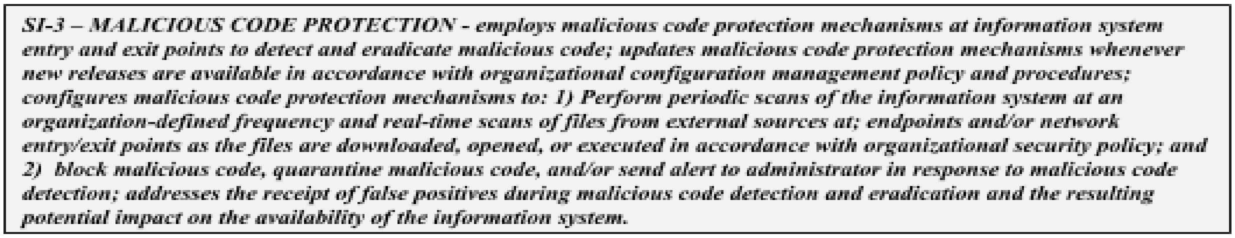
4.13 System and Information Integrity



SI-2 – FLAW REMEDIATION- The organization identifies, reports, and corrects information system flaws; tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within an organization-defined time period of the release of the updates; and incorporates flaw remediation into the organizational configuration management process.

Agencies should ensure that vendors of any components included in the FMIS have a well-defined process for identifying and remediating flaws in their component. To address flaws in deployed components, the flaw remediation process should be combined with a comprehensive plan for deploying secure updates and/or system patches to devices in the field.

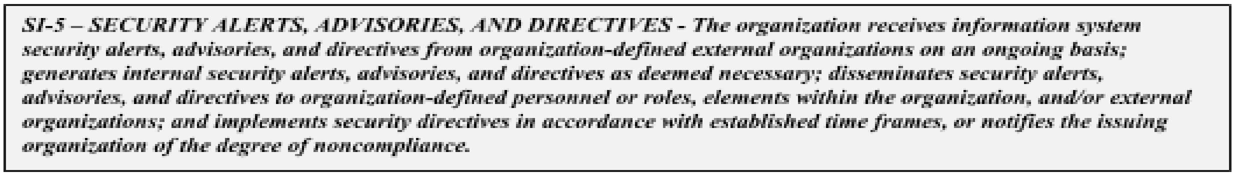
For further information refer to NIST SP 800-53 Rev 4 Control SI-2 supplemental guidance, NIST SP 800-147, NIST SP 800-155.



SI-3 – MALICIOUS CODE PROTECTION - employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; configures malicious code protection mechanisms to: 1) Perform periodic scans of the information system at an organization-defined frequency and real-time scans of files from external sources at; endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2) block malicious code, quarantine malicious code, and/or send alert to administrator in response to malicious code detection; addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Agencies should ensure that vendors employ mechanisms for ensuring protection of malicious code being introduced into components of the FMIS, such as through proper protection and configuration management of their source code, separation of duties, etc. Although the back-end system may appear to be more vulnerable to malicious code due to the nature of the system, i.e., use of common operating systems, access to the public networks, etc., agencies must ensure other components such as the telematics device are assessed. Several concerns with components such as the telematics device are its role interacting with the vehicle, the limited physical access to the device, and the presence of the entire operating system of the device being present in firmware. Agencies should ensure that the vendor of the component employs protection of the firmware to mitigate uploading of malicious code to the device.

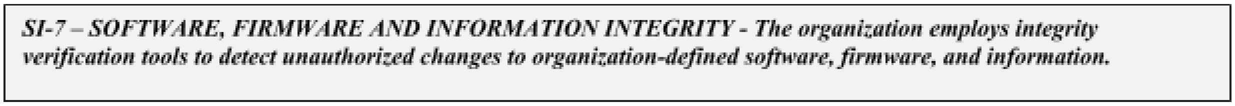
For further information refer to NIST SP 800-53 Rev 4 Control SI-3 supplemental guidance, NIST SP 800-83.



SI-5 – SECURITY ALERTS, ADVISORIES, AND DIRECTIVES - The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis; generates internal security alerts, advisories, and directives as deemed necessary; disseminates security alerts, advisories, and directives to organization-defined personnel or roles, elements within the organization, and/or external organizations; and implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Agencies should ensure personnel within their organization monitor industry and government resources that issue security alerts and advisories related to fleet management and vehicle systems., including resources such as NIST Common Vulnerabilities and Exposures (CVE), Bugtraq, etc.

For further information refer to NIST SP 800-53 Rev 4 Control SI-5 supplemental guidance, NIST SP 800-40.



SI-7 – SOFTWARE, FIRMWARE AND INFORMATION INTEGRITY - The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.

Agencies should ensure that vendors employ systems or processes to ensure the integrity of component software and firmware as well as the data recorded, managed, and stored by the system. As multiple vendors may be involved in the FMIS, it is likely that multiple entities will transfer government data via different systems and communications methods. Agencies should ensure that controls such as digital signatures for all software/firmware updates, host-to-host encryption, strong authentication, etc., are implemented to protect the integrity of the component software and firmware and of government data at all times.

For further information refer to NIST SP 800-53 Rev 4 Control SI-7 supplemental guidance, NIST SP 800-40, NIST SP 800-128

SI-10 – INPUT INFORMATION VALIDATION - The information system checks the validity of organization-defined information inputs.

Agencies should ensure that all components of the FMIS implement validity checking of all inputs. As the telematics device interfaces directly to the vehicle network, this is of significance important for program or processes validation. Agencies should ensure the vendor of a telematics device integrate processes or controls to limit commands or data transmitted to the vehicle network.

For further information refer to NIST SP 800-53 Rev 4 Control SI-10 supplemental guidance.

SI-16 – MEMORY PROTECTION - The information system implements organization-defined security safeguards to protect its memory from unauthorized code protection.

Agencies should ensure components employ industry-proven techniques to protect against unauthorized modification of software and hardware programs. Agencies should pay particular attention to components such as telematics devices that contain embedded systems. Embedded systems commonly store all code needed for operations within the device and as such are lucrative targets for malicious code. Agencies should ensure these types of components are protected from unauthorized modification of code by implementing protective mechanisms such as write protection.

For further information refer to NIST SP 800-53 rev 4 control SI-16 supplemental guidance.

5.0 Telematics Security Considerations

Although volumes of guidance, standards, and directives for securing information and information systems currently exist, there is no guidance specific to the protection or IA of vehicle automation and telematics systems. Ensuring the security posture of systems and products should always remain a high priority. However, in the absence of industry or government standards and guidance, agencies must be especially diligent in ensuring the IA posture of all components inherent in or incorporated into the vehicle as part of the FMIS.

Through collaborative endeavors, industry, academia, government, and professional organizations have initiated efforts to develop standards and best practices for the protection of both vehicles and telematics systems. Throughout the initial meetings and working groups related to these collaborative efforts, the following four subject areas have been the focus of concerns and in-depth discussions:

- Protecting communications between devices
- Protecting firmware on devices
- Protecting actions of devices
- Protecting integrity of devices

Within each of these subject areas, the working groups recommended that agencies look for the following security controls:

- **Protecting Communications Between Devices** – The groups recommended implementing encryption to protect all external communications, i.e. telematics to management system, management system to back-end data store, etc. Information and guidance available in publications such as NIST SP 800-52 Rev 1 for Transport Layer Security (TLS) as an example, are valuable resources available to aid the agency in assessing the use and implementation of encryption within the FMIS.
- **Protecting Firmware on Devices** – The groups recommended using both digital signatures and encryption to protect firmware on the devices, and to authenticate and protect the firmware update process. The group recommends cryptographically signing and encrypting firmware to prevent modification by an unauthorized entity. Information and guidance within NIST SP 800-53 Rev 4 Control SI-7 and Enhancements 1,2,6,9,10, 15 are valuable resources available to aid the agency in assessing the use of cryptographic signing and encrypting of communications and firmware. One common framework for applying secure updates is The Update Framework (TUF), an open, well-supported standard developed by New York University (NYU) for doing software updates, which is available at https://theupdateframework.github.io/. Also, DHS S&T, NYU, the University of Michigan Transportation Research Institute (UMTRI), and Southwest Research Institute (SwRI) have designed and implemented a Secure Over-the Air-Update (SOTA) prototype for automobiles called UPTANE. The open source code and documentation can be found at https://uptane.github.io/.
- **Protecting Actions on Devices** – The groups recommended implementing the principle of Least Privilege on all devices. The principle of Least Privilege is providing minimal privilege or rights to a user or process to enable it to operate for its desired function. The group also recommended configuring a device ONLY to support the functions necessary to satisfy the business need. Information and guidance within NIST SP 800-53 Rev 4 Control CM-7 and Enhancement 1 are a valuable resource to aid agencies in assessing the implementation of the principle of least privilege and limiting functionality. Agencies should keep in mind that adding of additional features introduces additional risk.
- **Protecting Integrity of Devices** – Finally, the groups recommended that manufacturers and/or maintainers of devices institute a vulnerability response program for receiving, implementing, and addressing vulnerabilities discovered or reported in their products. Vendors should maintain a vulnerability response and disclosure program in accordance with established standards such as International Organization of Standards (ISO)/International Electrotechnical Commission (IEC) 29147:2014 (Information technology -- Security techniques -- Vulnerability Disclosure) and ISO/IEC 30111:2013 (Information technology -- Security techniques -- Vulnerability Handling Processes). This is a valuable resource to aid agencies in assessing the implementation of a vulnerability response program.

The agency should not only report vulnerabilities they discover to the vendor(s) but also utilize procurement language that requires vendors have a vulnerability disclosure plan and program that meets or exceeds the ISO/IEC standards, as discussed above and also includes elements of the National Telecommunications and Information Administration (NTIA) Coordinated Vulnerability Disclosure Template. See Appendix A (Telematics Vulnerability Disclosure and Response Recommendations) for additional details and references to related documents that agencies can leverage for vulnerability handling and disclosure.

6.0 Summary

The security of the fleet management efficiency tool correlates directly to the overall security of the vehicle, user, and agency. A comprehensive approach to implementing cybersecurity controls is a significant contributing factor when selecting and implementing any FMIS. Agencies must remain aware and engaged of how agency assets are protected and agency fleet data is processed, accessed, managed, stored, and controlled through the use of the tool. Throughout the system lifecycle of the tool it is the responsibility of the fleet management office, as the system owner, to ensure the tool maintains a robust information security architecture in compliance with FISMA and agency guidelines. For compliance with FISMA guidelines it is the responsibility of the fleet management office, as the system owner, to coordinate authorization activities with the appropriate officials within their agency to ensure that the tool receives and maintains approval to operate within their agency throughout its lifecycle.

To assist agencies in developing and maintaining a robust information security architecture, NIST publishes guidance for designing and implementing information security concepts, procedures, policies, and controls. Agencies can find all the necessary information to assist them in procurement, development, configuration, operations, and maintenance of a secure information system within the volumes of guidance developed by NIST. The NIST SP 800 series documents will be cornerstones in developing and/or configuring the information security architecture baseline of the system. Throughout this document references have been made to the significance of the security recommendations within NIST SP 800-53, currently at Rev 4, and the importance of ensuring compliance with applicable controls when procuring and implementing a fleet management efficiency tool. As implementing security is not a 'one-size fits all' process, NIST provides guidance on implementing a Risk Management Framework (RMF) which allows for tailoring of security controls when establishing a robust information security architecture. Within this document references are made to specific individual controls. While the referenced controls are not inclusive of the security controls levied on government systems, the subset was selected based on their applicability in mitigating vulnerabilities seen in the current offerings of FMIS. The subset of security controls selected relate to:

- Enforcement of authentication and validation for all actions of the tool;
- Granting of minimal privileges to users/processes of the tool when performing required functions;
- Compliance with federal and agency mandates for all components of the tool;
- Enabling of only necessary service required for tool functionality;
- Protection of all communications of the tool;
- Capability of the tool to audit security related events;
- Ability to protection the tool against malicious code and activities;

- Ability to protect the integrity of the tool and data;
- Ability to limit communications between the tool and the vehicle;
- Ability to protect the integrity of software and software updating;
- Implementation or validation of a clear and concise vulnerability management process;
- Implementation of a comprehensive incident response process;
- Assessment of security throughout the supply chain of the tool;
- Documentation of all requirements and methods of access to/from the tool;
- Documentation of any function required to be performed without authentication;
- Documentation of any function required to be performed with elevated privileges;
- Categorization of the security level of data being processed;
- Categorization of the security level of the tool;
- Development of policies and procedures for secure configuration and operations of the tool;
- Conducting risk assessments of the tool, data, and processes;
- Coordination of third-party assessments of the tool;
- Ensuring agency authorization to operate the tool.

The prior listing should be considered as part of an overall assessment of the information security architecture of a FMIS. The full assessment of the tool should incorporate considerations for industry best practices as well as all security controls found in the NIST publications that are identified as applicable to the tool. Agencies must ensure a comprehensive information security architecture is addressed throughout the lifecycle of the tool and that the tool is capable of achieving and maintaining authorization for use within the agency.

Appendix A - Telematics Vulnerability Disclosure and Response Recommendations

Telematics vendors should have a coordinated vulnerability response and disclosure program which allows manufactures, operators, users, and researchers to report vulnerabilities discovered within the telematics device, or system. When security researchers discover a vulnerability in an organization's technology, the organization should have a process in place to work with the researcher to mitigate the vulnerability. Communication is an important part of a vendor's vulnerability response and disclosure program because it allows the vulnerability reporter to answer the vendor's questions while being informed about the vendor's solution to remediate the issue. If a vulnerability is discovered, the reporter should be aware of their own organization's disclosure policy before reporting an issue discovered in research, testing, or usage. There are three related initiatives that can be leveraged by agencies for vulnerability disclosure and handling:

- Two ISO standards, ISO/IEC 29147[6], and ISO/IEC 30111[7], contain best practices for vulnerability disclosure and handling
- To help foster this collaboration for safety-critical Internet of Things (IoT) systems, including automotive, the NTIA recently convened a multi-stakeholder process to address principles and practices around security researcher disclosure. The process is referred to as an "early stage" coordinated vulnerability disclosure template policy document which describes why security disclosure is important especially for safety-critical industries/systems such as those found in modern vehicles as well as an example of how a business can implement the template[8].
- NTIA in conjunction with the Forum of incident Response and Security Teams (FIRST) has compiled a collection of best practices entitled Guidelines and Practices for Multi-Party Vulnerability Coordination[9]. The document is a compendium of coordination resource documents and recommended methods for reporting and considers complex and typical real life scenarios that go beyond a single researcher notifying a single company.

The agency should not only report vulnerabilities discovered to the vendor(s) but also should through procurement language require that the vendor have a vulnerability disclosure plan and program that meets or exceeds the ISO/IEC standards, as discussed above and also includes elements of the NTIA Coordinated Vulnerability Disclosure Template.

[6] **ISO/IEC 29147:** *http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170*

[7] **ISO/IEC 30111:** *http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231*

[8] **NTIA:** *http://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf*

[9] **Vulnerability Management:** *http://www.first.org/global/sigs/vulnerability-coordination/multiparty*

Appendix B - References

DoD Instruction 8500.01, “Cybersecurity”, March 14, 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DoD Instruction 8551.01, “Identification (ID) Cards Required by the Geneva Conventions”, June 9, 2014. http://www.dtic.mil/whs/directives/corres/pdf/100001p.pdf

Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, March 25, 2016. https://www.gpo.gov/fdsys/pkg/FR-2015-03-25/pdf/2015-07016.pdf

FIPS Publication 140-2, “Security Requirements for Cryptographic Modules”, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems”, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

FISMA, “Federal Information Security Management Act”, December 2002. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

FISMA, “Federal Information Security Modernization Act”, December 18, 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

ISO/IEC 15408, “Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model”, December 2009. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341

ISO/IEC 15408, “Information technology -- Security techniques – Vulnerability and Handling Processes security”, November 2013. https://www.iso.org/standard/53231.html

ISO/IEC 15408, “Information technology -- Security techniques – Vulnerability Disclosure”, February 2014. https://www.iso.org/standard/45170.html

NTIA Safety Working Group, ““Early Stage” Coordinated Vulnerability Disclosure Template Version 1.1”, December 15, 2016. https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

NIST Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook”, October 1995. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf

NIST Special Publication 800-18, “Guide for Developing Security Plans for Federal Information Systems”, February 2006. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

NIST Special Publication 800-30, “Guide for Conducting Risk Assessments”, September 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST Special Publication 800-35, “Guide to Information Technology Security Services”, October 2003. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf

NIST Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems”, June 5,2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

NIST Special Publication 800-39, “Managing Information Security Risk”, March 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST Special Publication 800-40, “Guide to Enterprise Patch Management Technologies”, July 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

NIST Special Publication 800-41, “Guidelines on Firewalls and Firewall Policy”, September 2009. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

NIST Special Publication 800-46, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security”’ July 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

NIST Special Publication 800-48, “Guide to Securing Legacy IEEE 802.11 Wireless Networks”, July 2008. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf

NIST Special Publication 800-52, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”, April 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

NIST Special Publication 800-53A, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations”’ December 18, 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”, May 2013. http://dx.doi.org/10.6028/NIST.SP.800-56Ar2

NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”, September 2014. http://dx.doi.org/10.6028/NIST.SP.800-56Br1

NIST Special Publication 800-56C, “Recommendation for Key Derivation through Extraction-then-Expansion”, November 2011. http://dx.doi.org/10.6028/NIST.SP.800-56C

NIST Special Publication 800-57, “Recommendation for Key Management”,
Part 1: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 January 2016.
Part 2: http://dx.doi.org/10.6028/NIST.SP.800-57p2 August 2005.
Part 3: http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1 January 2015.
NIST Special Publication 800-61, “Computer Security Incident Handling Guide”, August 2012. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST Special Publication 800-70, “National Checklist Program for IT Products – Guidelines for Checklist Users and Developers”, December 8, 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r3.pdf

NIST Special Publication 800-77, “Guide to IPsec VPNs”, December 2005. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

NIST Special Publication 800-83, “Guide to Malware Incident Prevention and Handling for Desktops and Laptops”, July 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

NIST Special Publication 800-92, “Guide to Computer Security Log Management”, September 2006. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

NIST Special Publication 800-94, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, February 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

NIST Special Publication 800-95, “Guide to Secure Web Services”, August 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf

NIST Special Publication 800-97, “Establishing Wireless Robust Security Networks”, February 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

NIST Special Publication 800-121, “Guide to Bluetooth Security
“, June 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf

NIST Special Publication 800-128, “Guide for Security-Focused Configuration Management of Information Systems”, August 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-128.pdf

NIST Special Publication 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”, September 2011.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST Special Publication 800-147, “BIOS protection Guidelines”, April 2011.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

NIST Special Publication 800-155, “BIOS Integrity Measurement Guidelines (DRAFT)”, December 2011. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

NIST Special Publication 800-100, “Information Security Handbook: A Guide for Managers”, March 7, 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

NIST Special Publication 800-111, “Guide to Storage Encryption Technologies for End User Devices”, November 2007.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

NIST Special Publication 800-113, “Guide to SSL VPNs”, July 2008.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf

NIST Special Publication 800-115, “Technical Guide to Information Security Testing and Assessment”, September 2008.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf