EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OUI/DPM
	DATE November 2, 2020

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 4-21

TO: STATE WORKFORCE AGENCIES

FROM: JOHN PALLASCH
Assistant Secretary

SUBJECT: Unemployment Insurance (UI) Information Technology (IT) Security – Additional Information

1. **Purpose.** To provide State Workforce Agencies (SWAs) with information on the National Institute of Standards and Technology (NIST) IT security guidelines for use by SWAs to ensure the security of their UI IT systems.

2. **Action Requested.** The Employment and Training Administration (ETA) requests that state administrators provide this information, including the attached UI IT Security Guide, to the appropriate staff, including UI Directors and Chief Information Officers.

3. **Summary and Background.**

   a. Summary - In an ongoing effort to provide updates to the UI IT security information to the SWAs, this advisory transmits and provides the link to the UI IT Security Guide (https://ui.workforcegps.org/resources/2019/08/19/16/47/UI_IT_Security_Guide) on the UI Community of Practice (UI CoP) website.

   b. Background – It is critical to the integrity of the UI program that SWAs continuously improve the security of their UI IT systems. Since 2004, ETA has periodically provided security guidance to the SWAs. Unemployment Insurance Program Letter (UIPL) No. 24-04, and its Changes 1, 2, 3, 4, and 5 provided the SWAs with IT security guidance via a Compact Disk (CD), titled *IT Security Information.* With this UIPL, ETA has collaborated with the Department of Labor's Office of Chief Information Officer to provide an updated version of the UI IT Security Guide as an attachment to this UIPL.

4. **IT Security Guidance.** Conducting periodic IT security assessments and audits offer an opportunity for SWAs to ensure compliance with Federal requirements, to help receive the authority to operate from state authorities, connect to Federal systems to meet program requirements, and to identify and respond to areas where system security can be improved.

RESCISSIONS None	EXPIRATION DATE Continuing

ETA strongly encourages each SWA to conduct periodic IT security assessments and audits of its UI IT systems in accordance with the NIST IT security guidelines, specified in the NIST Special Publication (SP) 800-53A, and to take necessary steps to improve its IT security based on the results of the assessments. Additionally, ETA recommends the use of an "independent" entity to conduct state IT security assessments and audits as a best practice. The entity conducting the assessment or audit must be technically, managerially, and financially independent of the system that is under review.

The results of the security assessment can be used each year as a basis for providing an update on the assurance referenced in State Quality Service Plan Handbook 336, Chapter 1, Section VIII, J, Assurance of Automated Information System Security.

Each state is required to provide an assurance that it is maintaining adequate IT security and that such security is commensurate to the level of risk associated with the UI program and the UI IT environment. Given the massive quantities of personally identifiable information (PII) and confidential data maintained on state IT systems, it is critical that SWAs follow industry protocols for maximum IT security.

NIST IT security guidelines are based on best practices complied from several security documents, organizations, and publications, and are designed as a framework for Federal agencies and programs requiring stringent IT security measures. NIST SPs assist federal agencies to meet requirements mandated under the Federal Information Security Management Act (FISMA) and other regulations. The NIST IT security-related guidance is widely used by Federal agencies, and it offers a comprehensive security framework and guidance for SWAs to follow when implementing an information security program.

The UI IT Security Guide provides information for SWAs to conduct periodic security assessments and provides references to specific laws, regulations, and NIST SPs for IT security-related guidance. The security assessment guidelines are based on criteria and guidance established by NIST and specified in the SPs. SWAs may conduct a security assessment of their UI systems to verify that security controls conform to the laws, regulations, and the guidance established by NIST.

The following NIST publications are important for conducting security assessments of UI IT systems. The links to access these and other external publications are provided in the attached UI IT Security Guide.

- Federal Information Processing Standards (FIPS) Publication 199, which provides standards for categorizing information and information systems;
- FIPS Publication 200 and NIST SP 800-53, which provide guidelines for selecting and specifying security controls that meet minimum security requirements for information systems; and
- NIST SP 800-53A, which provides guidelines for assessing the effectiveness of security controls employed in information systems.

Protecting Personally Identifiable Information (PII)

Securing the confidentiality, integrity, and availability of information stored in SWA UI IT systems is vital to controlling fraud in the UI program. Recent Office of Inspector General investigations have identified that, in some situations, state employees abused their positions of trust by misusing confidential PII to enable UI fraud. The NIST SP 800-53, Personnel Security (PS) security control (Position Risk Designation (PS-2) and Personnel Screening (PS-3)), provides guidance on controls that should be followed prior to assigning personnel handling PII. ETA recommends that SWAs conduct pre-employment and periodic background and credit checks for employees with direct access to PII related to the UI program and take appropriate actions with employees who have negative results related to periodic suitability investigations in accordance with NIST SP 800-53. Additionally, SWAs should strengthen existing systematic audit controls to track access to PII.

ETA strongly recommends that SWAs implement the following security controls in accordance with the guidance provided in NIST SP 800-53 to protect PII:

- Access Control;
- Awareness and Training;
- Audit and Accountability;
- Identification and Authentication;
- Individual Participation;
- Physical and Environmental Protection; and
- Personnel Security.

Additionally, NIST SP 800-122 provides specific guidance that SWAs can use in protecting the confidentiality of PII, including how to prevent inappropriate access, use, and disclosure of this information. This SP provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The guide also suggests safeguards that may offer appropriate levels of protection for PII.

Preventing Cyber Threats and Attacks on Critical Infrastructure

Cyber-attacks on digital and physical infrastructure systems are growing areas of concern. These threats are escalating as more sophisticated, organized groups are designing targeted attacks to damage or disrupt vital services and critical physical systems. The National Infrastructure Advisory Council is tasked with assessing how existing Federal authorities and capabilities can be employed to assist and better support the cybersecurity of critical infrastructure assets that are at greatest risk of a cyber-attack, possibly resulting in catastrophic regional or national effects on public health or safety, economic security, or national security.[1]

[1] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017.

SWAs are strongly encouraged to protect their IT systems and information from cyber-attacks such as viruses, trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information), and control system attacks. The Cybersecurity Infrastructure Security Agency (CISA), a division of the Department of Homeland Security, is responsible for protecting the nation's critical infrastructure from physical and cyber threats. CISA's website provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders. SWAs should use available guidance and resources provided by CISA to implement a cybersecurity program. For example, there have been recent ransomware attacks on state and county governments, a type of virus that can compromise the computer networks across agencies. A ransomware attack typically locks an infected computer system until payment, usually in the form of cryptocurrency, is sent to the hacker. CISA provides information on how to protect IT systems from ransomware attacks, and how to respond to possible ransomware attacks. See Cybersecurity and Infrastructure Security Agency Ransomware at https://www.us-cert.gov/Ransomware.

Incident Reporting

Computer security incident response has become an important component of IT programs. Cybersecurity-related attacks have become more numerous and diverse as well as more damaging and disruptive. New types of security-related incidents emerge frequently; therefore, preventive activities based on the results of risk assessments can help to minimize these types of incidents. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

States are encouraged to implement formal procedures for Incident Reporting using NIST SP 800-61 that provides guidelines for incident handling including data breaches, particularly for analyzing incident-related data and determining the appropriate response for each incident. Additionally, while states may have their own security breach notification laws that require them to notify individuals or entities affected by a data breach and take specific steps to remedy the situation, SWAs are encouraged to periodically review and enhance their notification procedures using best practices and other guidance provided in NIST SP 800-122. This publication provides recommendations for developing incident response plans for breaches involving PII.

UI Information Technology Support Center (ITSC)

UI ITSC provides SWAs with the full scope of IT Security guidance as part of its UI IT Modernization support and delivery, as well as the application of FIPS, FISMA, NIST, and Internal Revenue Service (IRS) Publication-1075 standards. UI ITSC IT Security-related services includes collaborating with SWAs for the development of a System Security Plan, assisting in remediation of System Security Plan deficiencies and addressing SWA Security Audit findings. UI ITSC provides guidance to SWAs in NIST-driven areas such as Contingency Planning, Auditing, Continuous Monitoring, FIPS-140-2 Encryption, and Configuration Management.

With the growing emphasis of the use of the Cloud technology in the UI Domain, UI ITSC provides expert advice on Cloud preventative, detection, countermeasure, and remediation security Cloud services. UI ITSC has worked very closely with SWAs who were early Cloud technology adopters, especially emphasizing Social Security Administration (SSA) security requirements for accessing SSA data and IRS Publication-1075 standards for cloud compliance and safeguards for the Treasury Offset Program[2]implementation.

UI ITSC has IT Security-related resources on its members only website, www.itsc.org. SWAs can contact UI ITSC at securitycorner@itsc.org for IT Security guidance and services.

5. **Inquiries.** Please direct inquiries to the appropriate ETA Regional Office or to Jagruti Patel, 202-693-3059, patel.jagruti@dol.gov in the National Office**.**

6. **References.**
   - Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017;
   - UIPL No. 24-04, *Unemployment Insurance Information Technology Security*, and its Changes 1, 2, 3, 4, and 5, https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=1575;
   - ET Handbook No. 336, 18th Edition, *Unemployment Insurance (UI) State Quality Service Plan (SQSP) Planning and Reporting Guidelines, Chapter 1, Section VIII, J, Assurance of Automated Information Systems Security*, https://wdr.doleta.gov/directives/attach/ETAHandbook/ETHand336_18th_Ch3.pdf?DOCN=2831;
   - FIPS Publication 199, *Standards for Security Categorizations of Federal Information and Information Systems*;
   - FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
   - NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*;
   - NIST SP 800-53A, *Assessing the Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*;
   - NIST SP 800-61, *Computer Security Incident Handling Guide*; and
   - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

7. **Attachment.** UI IT Security Guide

[2] The Treasury Offset Program is a centralized offset program, administered by the Bureau of the Fiscal Service's Debt Management Services (DMS), to collect delinquent debts owed to federal agencies and states (including past-due child support), in accordance with 26 U.S.C. § 6402(d) (collection of debts owed to federal agencies), 31 U.S.C. § 3720A (reduction of tax refund by amount of the debts), and other applicable laws.

UNEMPLOYMENT INSURANCE

IT Security Guide

July 2020

Table of Contents

UI Information Technology Security

State Workforce Agencies (SWAs) rely on information technology (IT) to administer their Unemployment Insurance (UI) systems. With a growing complexity of IT infrastructure, and a constantly changing information security threat and risk environment, information security has become a mission-essential function. This function should be managed and governed to reduce the risks to the SWAs' operations; to ensure the security of the confidential data in SWA UI IT systems; and to ensure the SWAs' ability to do business and serve the American public.

SWAs are required to provide assurance that they have taken the necessary steps to secure their computer systems as outlined in the State Quality Service Plan (SQSP) Planning and Reporting Guidelines[1] . SWAs have an obligation to provide adequate security of their UI IT systems as part of their administration of the UI program. Failure to provide adequate security could result in unpredicted system failures and malicious attacks leading the public to lose trust in the agencies' ability to perform necessary and critical functions. It may also lead to data breaches of PII that compromises individuals' identities and confidential data.

As required in federal law, the National Institute of Standards and Technology (NIST) develops and maintains an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information system in the Federal Government. NIST developed its Special Publications (SP) 800 series to address and support the security and privacy needs of federal agencies' information and information systems. The material provided in this document is based on NIST standards and guidelines.

An effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each organizational information system;
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the

[1] Reference to ET HANDBOOK NO. 336, 18th Edition, Chapter I, section VIII – Assurances, sub-section J. that lists the state's requirement in ensuring its automated information systems is secure.

information security risks associated with their activities and their responsibilities for complying with organizational policies and procedures designed to reduce these risks;

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents;
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization; and
- Procedures to implement multifactor authentication (MFA) to protect users against hacking attacks and social engineering. Even if a hacker obtains a user's password, they cannot access the user's data unless the hacker also has the second component of MFA.

Potential risks of not addressing security of the UI working environment include:

- UI operations and customer service delivery may suffer.
- UI Benefit or Tax records could be altered, deleted, or corrupted.
- SWAs may fail timeliness, quality or accuracy performance measures.
- Inappropriate and/or fraudulent payments may occur.
- The UI IT internal/external networks could be vulnerable to exploitation.
- The UI IT environment could crash and/or be damaged.
- The public and employer communities may lose confidence in the UI program.
- Negative political and/or legal consequences could ensue.
- UI personnel may lose their job.

Purpose

The purpose is to assemble information necessary to develop, implement and assess the security of the UI IT systems. In addition, the purpose is to provide guidance to ensure that SWAs proactively implement appropriate information security controls to support their mission in a cost-effective manner while managing evolving information security risks. To ensure an appropriate level of support of agency missions and the proper implementation of current and future information security requirements, each agency should establish a formal information security governance structure. Information security governance has its own set of requirements, challenges, activities, and types of possible structures. Information security governance also has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities.

Intended Audience

The intended audience for this guidance includes the UI managers and IT staff who support the UI program, and/or support the SWA's efforts in carrying out the UI program. The intent is to provide a method for agency officials to determine the current status of their information security program so that improvements can be incorporated and implemented to their UI program to provide security commensurate with the level of risk associated with UI operations and the UI IT work environment.

As a starting point for managers, the guidance document, NIST SP 800-100, *Information Security Handbook: A Guide for Managers* provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Security Standards

Security Standards, such as Federal Information Processing Standards (FIPS), are standards developed by the United States Federal Government for use in computer systems by non-military government agencies. The purpose of FIPS is to ensure that the Federal Government agencies adhere to the same guidelines regarding IT security.

NOTE: FIPS Publications, that are important to the SQSP IT Security Assurances, have been denoted by a * symbol. Two key FIPS Security Standards include:

- ***FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems***, directs federal agencies categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high-water mark concept must be used to determine the overall impact level of the information system. Thus, a low-impact system is an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. Finally, a high-impact system is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.
- ***FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems***, specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. This standard will promote the development, implementation, and operation of more secure information systems by establishing minimum

levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

- **FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors***, specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and logical access to government information systems. This standard contains the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive-12 [HSPD-12], including identity proofing, registration, and issuance.
- ***Federal Risk and Authorization Management Program (FedRAMP)*** is a government-wide program to standardize how the Federal Information Security Management Act (FISMA) applies to cloud computing services. It provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

  This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies and cloud service providers (CSPs).

Minimum Security Requirements

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* provides guidelines for selecting and specifying security controls to protect organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The minimum security requirements cover 18 security-related areas with regard to protecting the confidentiality, integrity, and availability of the information systems and the information processed, stored, and transmitted by those systems. The 18 areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the information and information systems.

1. **Access Control (AC):** Organizations must limit: (i) system access to authorized users; (ii) processes acting on behalf of authorized users; (iii) devices, including other systems; and (iv) types of transactions and functions that authorized users are permitted to exercise. NIST SP 800-12, 800-46, 800-77, 800-94, 800-97, 800-100, 800-113, 800-114, and 800-124 provide guidance for effective implementation of AC-related security controls.
2. **Awareness and Training (AT):** Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their

assigned information security-related duties and responsibilities. NIST SP 800-12, 800-16, 800-50, and 800-100 provide guidance for effective implementation of AT-related security controls.

3. **Audit and Accountability (AU):** Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. NIST SP 800-92 provides guidance for effective implementation of AU-related security controls.
4. **Assessment, Authorization, and Monitoring (CA):** Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. NIST SP 800-12, 800-37, 800-39, 800-47, 800-53A, 800-100, 800-115, and 800-137 provide guidance for effective implementation of CA-related security controls.
5. **Configuration Management (CM):** Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems. NIST SP 800-12, 800-70, 800-100, and 800-128 provide guidance for effective implementation of CM-related security controls.
6. **Contingency Planning (CP):** Organizations must: (i) establish, maintain, and effectively implement plans for emergency response, (ii) back up operations, and (iii) oversee post-disaster recovery for organizational systems to ensure the availability of critical information resources and the continuity of operations in emergency situations. NIST SP 800-12, 800-16, 800-34, 800-50, 800-84, and 800-100 provide guidance for effective implementation of CP-related security controls.
7. **Identification and Authentication (IA):** Organizations must: (i) identify system users, processes acting on behalf of users, or devices and (ii) authenticate or verify the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. NIST SP 800-12, 800-63, 800-73, 800-76, 800-78, 800-100, and 800-116 provide guidance for effective implementation of IA-related security controls.
8. **Incident Response (IR):** Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities. NIST SP 800-12, 800-16, 800-50, 800-61, 800-83, 800-84, 800-100, and 800-115 provide guidance for effective implementation of IR-related security controls.

9. **Maintenance (MA):** Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. NIST SP 800-12, 800-63, 800-88, and 800-100 provide guidance for effective implementation of MA-related security controls.
10. **Media Protection (MP):** Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. NIST SP 800-12, 800-56, 800-57, 800-60, 800-88, 800-100, and 800-111 provide guidance for effective implementation of MP-related security controls.
11. **Physical and Environmental Protection (PE):** Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems. NIST SP 800-12, 800-46, 800-73, 800-76, 800-78, 800-100, and 800-116 provide guidance for effective implementation of PE-related security controls.
12. **Planning (PL):** Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. NIST SP 800-12, 800-18, 800-37, and 800-100 provide guidance for effective implementation of PL-related security controls.
13. **Program Management (PM):** Program Management controls include: information security program plan, information security resources, plan of action and milestone process, system inventory, enterprise architecture, risk management strategy, insider threat program, and threat awareness program. NIST SP 800-16, 800-30, 800-37, 800-39, 800-53A, 800-55, 800-60, and 800-137 provide guidance for effective implementation of PM-related security controls.
14. **Personnel Security (PS):** Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures. NIST SP 800-12, 800-35, 800-60, 800-73, 800-76, 800-78, and 800-100 provide guidance for effective implementation of PS-related security controls.
15. **Risk Assessment (RA):** Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information. NIST SP 800-12,

800-30, 800-39, 800-40, 800-60, 800-70, 800-100, and 800-115 provide guidance for effective implementation of RA-related security controls.

16. **System and Services Acquisition (SA):** Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization. NIST SP 800-12, 800-35, 800-37, 800-53, 800-53A, 800-60, 800-70, 800-100, 800-128, and 800-137 provide guidance for effective implementation of SA-related security controls.

17. **System and Communications Protection (SC):** Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. NIST SP 800-12, 800-28, 800-32, 800-41, 800-52, 800-56, 800-57, 800-58, 800-63, 800-77, 800-81, 800-95, 800-100, 800-111, and 800-113 provide guidance for effective implementation of SC-related security controls.

18. **System and Information Integrity (SI):** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response. NIST SP 800-12, 800-40, 800-45, 800-61, 800-83, 800-92, 800-94, 800-100, 800-128, 800-137, and 800-147 provide guidance for effective implementation of SI-related security controls.

Security Controls Selection

Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by agency officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective in their application?

The answers to these questions are not given in isolation but rather in the context of an effective information security program for the organization that identifies, controls, and mitigates risks to its information and information systems.

The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the organization.

The selected set of security controls must include one of three appropriately tailored security control baselines from NIST SP 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- For low-impact information systems, organizations must, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.
- For moderate-impact information systems, organizations must, as a minimum, employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
- For high-impact information systems, organizations must, as a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

The resulting set of security controls must be documented in the security plan for the information system. The application of the security controls defined in NIST SP 800-53 required by this standard represents the current state-of-the-practice safeguards and countermeasures for information systems. Security controls must include multiple layer/staff sign-off for any system/programming changes to ensure that the system cannot be compromised.

Security Assessment

Security control assessments provide a line of defense in knowing the strengths and weaknesses of an organization's information system. Security controls assessment determines whether security controls in an information system are operating as intended. The results of this assessment are used in determining the overall effectiveness of the security controls in an information system, identifying residual vulnerabilities in the system, providing credible and meaningful inputs to the organization's Plan of Action and Milestones.

SWAs are encouraged to perform internal IT Security Assessments and to have independent IT Security entities to conduct impartial assessments of their UI IT systems. The independent assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the system under assessment or to the determination of security control effectiveness.

NIST SP 800-53A *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* provides guidelines for assessing the effectiveness of security controls employed in information systems. Guidelines apply to the security controls defined in NIST SP 800-53. The guidelines have been developed to help achieve more secure information systems by:

- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating cost-effective assessments of security control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, or individuals resulting from the operation of information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support security accreditation decisions and FISMA compliance.

The assessment procedures catalog can be used as a starting point for developing comprehensive security assessment plans to support a variety of potential assessment activities associated with determining the effectiveness of security controls in organizational information systems.

Organizations have flexibility in determining which controls, and how many controls are assessed annually, provided all security controls applicable to the information system are assessed over the course of the system accreditation period.

A well-executed security controls assessment validates the security controls contained in the information system security plan and facilitates a cost-effective approach to correcting deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

Laws

This section gives a brief, high-level overview of the different laws that are used to provide standards in providing computer security.

- **Clinger-Cohen Act** This Act requires agencies to establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all of its major investments in information systems. It also requires that agencies ensure that the information security policies, procedures, and practices are adequate. The selection of information technology should be integrated with the process for making budget, financial, and program management decisions within the agency.
- **Federal Information Security Management Act of 2002** The FISMA requires federal agencies to assess the security of their non-classified information systems providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. More important from an enforcement perspective, the law requires every agency to provide a risk assessment and report the security needs of its systems. These must be included in every agency budget request. FISMA

enforces accountability and requires each agency to examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports.

- **Federal Information Security Modernization Act of 2014** was an amendment to FISMA that made several modifications to modernize federal security practices as well as promote and strengthen the use of continuous monitoring.
- **Cybersecurity and Infrastructure Security Agency Act of 2018** elevates the mission of the former Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) and establishes the Cybersecurity and Infrastructure Security Agency (CISA). CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats, a mission that requires effective coordination and collaboration among a broad spectrum of government and private sector organizations, to build a more secure and resilient infrastructure for the future. The CISA website provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the Nation's essential resources.

Regulations

This section briefly explains the Office of Management and Budget (OMB) Circular No. A-130, Appendix III and the Federal Information System Control Audit Manual (FISCAM).

- **OMB Circular No. A-130, Appendix III: Security of Federal Automated Information Resources** Appendix III of the Office of Management and Budget Circular Number A-130 establishes a minimum set of controls to be included in federal automated information security programs. This directive lists and explains the four controls and the sub-tasks of each control that must be incorporated when operating a general support or major application computer system. The Appendix provides definitions to the terms adequate security, application, general support system, and major application, terms that must be applied when setting up the necessary controls on computer systems.
- **Federal Information System Control Audit Manual (FISCAM)** FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards. FISCAM control activities are consistent with NIST Special Publication 800-53 and all SP800-53 controls have been mapped to the FISCAM.
- The FISCAM, which is consistent with NIST, is organized to facilitate effective and efficient IS control audits. Specifically, the methodology in the FISCAM incorporates the following:
  - Top-down, risk-based approach that considers materiality and significance in determining effective and efficient audit procedures and is tailored to achieve the audit objectives.
  - Evaluation of entity-wide controls and their effect on audit risk.
  - Evaluation of general controls and their pervasive impact on business process application controls.

- Evaluation of security management at all levels (entity-wide, system, and business process application levels).
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses
- Groupings of control categories consistent with the nature of the risk.
- Experience gained in U. S. General Accounting Office's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

FISCAM Information Security Controls

IS controls consist of those internal controls that are dependent on information systems processing and include general controls (entity-wide, system, and business process application levels) and business process application controls (input, processing, output, master file, interface, and data management system controls).

General Controls

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

- **Security Management** – Controls provide reasonable assurance that security management is effective, including:
  - security management program
  - periodic assessments and validation of risk,
  - security control policies and procedures,
  - security awareness training and other security-related personnel issues,
  - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
  - remediation of information security weaknesses, and
  - security over activities performed by external third parties.
- **Access Controls** – Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable, restricted to authorized individuals, and includes effective
  - protection of information system boundaries,
  - identification and authentication mechanisms,
  - authorization controls,
  - protection of sensitive system resources,
  - audit and monitoring capability, including incident handling, and
  - physical security controls.
- **Configuration Management** – Controls provide reasonable assurance that changes to information system resources are authorized, systems are configured and operated securely and as intended, and includes effective
  - configuration management policies, plans, and procedures,

- current configuration identification information,
- proper authorization, testing, approval, and tracking of all configuration changes,
- routine monitoring of the configuration,
- timely software updates to protect against known vulnerabilities, and
- documentation and approval of emergency changes to the configuration.

- **Segregation of Duties** – Controls provide reasonable assurance that includes effective
  - segregation of incompatible duties and responsibilities and related policies, and
  - control of personnel activities through formal operating procedures, supervision, and review.

- **Contingency Planning** – Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, and includes effective
  - assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
  - steps taken to prevent and minimize potential damage and interruption,
  - comprehensive contingency plan, and
  - periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

Business Process Controls

Business process application controls are directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, confidential, and available.

- **Completeness –** controls provide reasonable assurance that all transactions that occurred are entered into the system, accepted for processing, processed once and only once by the system, and properly included in output.

- **Accuracy** – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements entered for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

- **Validity** – controls provide reasonable assurance that (1) all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) output contains only valid data.

- **Confidentiality** – controls provide reasonable assurance that application data, reports, and other output are protected against unauthorized access.

- **Availability** – controls provide reasonable assurance that application data, reports, and other relevant business information are readily available to users when needed.

NIST Special Publications

The NIST SP 800 series present information of interest to the computer security community. NIST develops SP 800 series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq*., Public Law (P.L.) 113-283. The NIST SPs are resources available to SWAs to help increase their knowledge and understanding of implementing security measures on their UI IT systems.

NIST SPs encompass all aspects of IT systems, some of which are not conducive to the UI SWA environment. This guidance only presents what is deemed appropriate to the UI environment.

NOTE: NIST Special Publications that are key to the SQSP IT Security Assurances have been denoted by a * symbol.

- **Special Publication 800-12 Revision 1: *An Introduction to Information Security: The NIST Handbook*** provides a high-level overview of information security principles by introducing related concepts and the security control families (as defined in NIST SP 800-53) that organizations can leverage to effectively secure their systems and information. To better understand the meaning and intent of the security control families described later, this publication begins by familiarizing the reader with various information security principles. After the introduction of these security principles, the publication provides detailed descriptions of multiple security control families as well as the benefits of each control family.
- **Special Publication 800-16: *Information Technology Security Training Requirements: A Role and Performance-Based Model*** explores the people factor in maintaining adequate information security. This document describes information technology/cyber security role-based training for federal departments and agencies. Its primary focus is to provide a comprehensive yet flexible training methodology for developing training courses or modules for personnel who have been identified as having significant information technology/cyber security responsibilities. Organizations need to have a training program to ensure every individual is aware of his/her requirements for information security.
- ***Special Publication 800-18 Revision 1: *Guide for Developing Security Plans for Federal Information Systems*** provides a recommended format for organizations to use in developing their system security plan. Although not mandatory, the format provides a standardized approach that simplifies plan development. The level of detail included within the plan should be consistent with the criticality and value of the system to the organization's mission. The system security plan should fully identify and describe the controls currently in place or planned for the system and should include a list of rules of behavior.
- ***Special Publication 800-30 Revision 1: *Guide for Conducting Risk Assessments*** provides guidance for conducting risk assessments of the information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk-management process, providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance

for carrying out each of the steps in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and explains how risk assessments and other organizational risk management processes complement and inform each other. Special Publication 800-30 also provides guidance to organizations on identifying specific risk factors to monitor on an ongoing basis so that organizations can determine whether risks have increased to unacceptable levels (i.e., exceeding organizational risk tolerance) and different courses of action should be taken.

- *Special Publication 800-34 Revision 1: *Contingency Planning Guide for Federal Information Systems* provides guidelines to organizations for preparing and maintaining information system contingency plans (ISCPs). The document discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of information system platforms, and provides examples to help readers develop their own ISCPs. It also provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle (SDLC). It also helps personnel evaluate information systems and operations to determine appropriate contingency planning requirements and priorities.

- Special Publication 800-35: *Guide to Information Technology Security Services* provides assistance with the selection, implementation, and management of IT security services by guiding organizations through the various phases of the IT security services life cycle. This life cycle provides a framework that enables the IT security decision makers to organize their IT security efforts from initiation to closeout. Failure to consider the many issues involved and to manage the organizational risks can seriously impact the organization. IT security decision makers should think about the costs involved and the underlying security requirements, as well as the potential impact of their decisions, on the organizational mission, operations strategic functions, personnel, and service provider arrangements.

- Special Publication 800-37 Revision 2: *Risk Management Framework for Information Systems and Organizations* provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. The guidelines have been developed:
  - To ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and risk management strategy established by the senior leadership through the risk executive (function);
  - To achieve privacy protections for individuals and security protections for information and information systems through the implementation of appropriate risk response strategies;
  - To support consistent, informed, and ongoing authorization decisions, reciprocity, and the transparency and traceability of security and privacy information; and

- To facilitate the integration of security and privacy requirements and controls into the enterprise architecture, SDLC processes, acquisition processes, and systems engineering processes.

- **Special Publication 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View*** is the flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA. The purpose of this publication is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. SP 800-39 provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.

- **Special Publication 800-40 Revision 3: *Guide to Enterprise Patch Management Technologies*** provides guidance on the basics of enterprise patch management technologies. This publication is based on the assumption that the organization has a mature patch management capability and is focused on increasing its automation level. Organizations that are seeking more basic guidance on establishing patch management programs or have legacy needs that cannot be met with current enterprise patch management technologies should, in addition to reading this publication, also consult the previous complementary version, SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*.

- **Special Publication 800-41 Revision 1: *Guidelines on Firewalls and Firewalls Policy*** provides information about firewall technologies and firewall policy primarily to assist those responsible for network security. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments. It also contains numerous recommendations for choosing, configuring, and maintaining firewalls.

- **Special Publication 800-44 Version 2: *Guidelines on Securing Public Web Servers*** recommends security practices for designing, implementing, and operating publicly accessible Web servers, including related network infrastructure issues. It helps in enhancing security on existing and future Web server systems to reduce the number and frequency of Web-related security incidents.

- **Special Publication 800-45 Version 2: *Guidelines on Electronic Mail Security*** recommends security practices for designing, implementing, and operating email systems on public and private networks. Attackers frequently target mail servers. Various types of email content and attachments have also proven to be effective in introducing viruses and other malware into networks through mail clients. Email is used extensively as a vector to deliver attacks that exploit vulnerabilities in users' workstations or social engineering methods intended to trick users. These attacks often lead to the compromise of user workstations or the release of sensitive information even when the email client is securely configured. This document may be

used by organizations interested in enhancing security on existing and future mail systems to reduce the number and frequency of email-related security incidents.

- **Special Publication 800-46 Revision 2: *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*** assists organizations in mitigating the risks associated with the enterprise technologies used for telework, such as remote access servers, telework client devices (including bring-your-own-device [BYOD] and contractor, business partner, and vendor-controlled client devices, also known as third-party-controlled devices), and remote access communications. The document emphasizes the importance of securing sensitive information stored on telework devices and transmitted through remote access across external networks. This document provides recommendations for creating telework-related policies and for selecting, implementing, and maintaining the necessary security controls for remote access servers and clients.

- **Special Publication 800-47: *The Security Guide for Interconnecting Information Technology Systems*** provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different organizations. This document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection. It also contains guides and samples for developing Interconnection Security Agreements (ISA) and a Memorandum of Understanding/Agreement (MOU/A). Finally, this document contains a guide for developing a System Interconnection Implementation Plan, which defines the process for establishing the interconnection, including scheduling and costs.

- **Special Publication 800-50: *Building an Information Technology Security Awareness and Training Program*** provides guidelines for building and maintaining a comprehensive awareness and training program as part of an organization's IT security program. The guidance is presented in a life-cycle approach, ranging from designing, developing, and implementing an awareness and training program through post-implementation evaluation of the program. The document includes guidance on how IT security professionals can identify awareness and training needs, develop a training plan, and get organizational buy-in for the funding of awareness and training program efforts.

- **Special Publication 800-53 Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations*** provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components of an information system that process, store, or transmit federal information.

- **Special Publication 800-53A Revision 4: *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*** provides: (i) guidelines for building effective security assessment plans and privacy assessment plans; and (ii) a comprehensive set of procedures for assessing the effectiveness of security controls and

privacy controls employed in information systems and organizations supporting the executive agencies of the Federal Government. The guidelines apply to the security and privacy controls defined in NIST SP 800-53.

- **Special Publication 800-55 Revision 1: *Performance Measurement Guide for Information Security*** is intended to be a guide for the specific development, selection, and implementation of IT system-level metrics to be used to measure the performance of information security controls and techniques. The requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons. The document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

- **Special Publication 800-58: *Security Considerations for Voice Over IP Systems*** is intended to provide agencies with guidance for establishing secure Voice Over Internet Protocol (VOIP) networks. VOIP refers to the transmission of speech across data-style networks. VOIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. This publication introduces VOIP, its security challenges, and potential countermeasures for VOIP vulnerabilities. VOIP security considerations for the public switched telephone network are largely outside the scope of this document.

- **Special Publication 800-60 Volume 1 Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*** addresses the FISMA direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact. The guideline facilitates application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system. This guideline assumes that the user is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standard [FIPS] 199).

- **Special Publication 800-61 Revision 2: *Computer Security Incident Handling Guide*** helps organizations mitigate the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents. Organizations are encouraged to tailor the recommended guidelines and solutions to meet their specific security and mission requirements.

- **Special Publication 800-63-3: *Digital Identity Guidelines*** provides an overview of general identity frameworks using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels.

- **Special Publication 800-67 Revision 2: *Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher*** specifies the TDEA block cipher. Data that is determined by a responsible authority to be sensitive, data that has a high value, or data that represents a high value should be protected cryptographically if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. This recommendation provides a description of a mathematical algorithm for cryptographically protecting binary coded information (e.g., using encrypt and authentication).
- **Special Publication 800-70 Revision 4: *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*** describes the use, benefits, and management of checklists and explains how to use the NIST National Checklist Program (NCP) to find and retrieve checklists. This publication also describes the policies, procedures, and general requirements for participation in the NCP.
- **Special Publication 800-73-4: *Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation*** specifies the PIV data model, application programming interface (API), and card interface requirements necessary to comply with the use cases as defined in Section 6 of FIPS 201 and further described in this publication. SP 800-73-4 contains the technical specifications to interface with the smart card to retrieve and use the identity credentials.
- **Special Publication 800-76-2: *Biometric Specifications for Person Identity Verification*** contains technical specifications for biometric data mandated or allowed in FIPS 201. These specifications reflect the design goals of interoperability, performance, and security of the PIV Card and PIV processes. This specification addresses iris, face, and fingerprint image acquisition to variously support background checks, fingerprint template creation, retention, and authentication.
- **Special Publication 800-77: *Guide to IPsec VPNs*** helps organizations mitigate risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec). This document presents information that is independent of particular hardware platforms, operating systems, and applications other than providing real-world examples to illustrate particular concepts. Specifically, the document includes a discussion of the need for network layer security services, a description of the types of services that are offered at the network layer, and explains how IPsec addresses these services. It also describes alternatives to IPsec and discusses the circumstances in which each alternative may be appropriate.
- **Special Publication 800-78-4: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*** publication encompasses the PIV card, infrastructure components that support issuance and management of the PIV card, and applications that rely on the credentials supported by the PIV card to provide security services. This publication identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, key establishment schemes, and message digest algorithms, and specifies mechanisms to identify the algorithms associated with PIV keys or digital signatures.

- **Special Publication 800-83 Revision 1: *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*** helps a wide variety of organizations understand the threats posed by malware and mitigate the risks associated with malware incidents. In addition to providing background information on the major categories of malware, it provides practical, real-world guidance on preventing malware incidents and responding to malware incidents in an effective, efficient manner.
- **Special Publication 800-84: *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*** provides guidance on designing, developing, conducting, and evaluating Test, Training, and Exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events that may affect their missions. The scope of this document is limited to TT&E events for single organizations, as opposed to large-scale events involving multiple organizations, involving internal IT operational procedures for emergencies. This document does not address TT&E for a specific type of IT plan; rather, the TT&E methodology described in this document can be applied to TT&E events built around any IT plan or around an IT emergency-handling capability that is not necessarily documented in a plan, such as computer security incident response.
- **Special Publication 800-86: *Guide to Integrating Forensic Techniques into Incident Response*** helps organizations investigate computer security incidents and troubleshoot some IT operational problems by providing practical guidance on analyzing data from computers and networks. Specifically, the document includes a description of the sources, including files, operating systems, network traffic, and applications. This guide provides general recommendations for performing the data analysis process. It also provides detailed information on using the process with four major categories of data sources: files, operating systems, network traffic, and applications. The guide focuses on explaining the basic components and characteristics of data sources within each category, as well as techniques for the acquisition and examination of data from each category. The guide also provides recommendations for how multiple data sources can be used together to gain a better understanding of an event.
- **Special Publication 800-88 Revision 1: *Guidelines for Media Sanitization*** helps organizations implement a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality. The objective of this special publication is to aid decision making when media require disposal or reuse, or will leave the effective control of an organization. The information in this guide is best applied in the context of current technology and applications. It also provides guidance for information disposition, sanitization, and control decisions to be made throughout the system life cycle.
- **Special Publication 800-92: *Guidelines to Computer Security Log Management*** helps organizations understand the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers

several topics, including establishing log management infrastructures and developing and performing robust log management processes throughout an organization. The publication presents log management technologies from a high-level viewpoint. It is not a step-by-step guide to implementing or using log management technologies.

- **Special Publication 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS)*** helps organizations understand intrusion detection system and intrusion prevention system technologies and designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention system (IDPS) solutions. It provides practical, real-world guidance for each of four classes of IDPS products: network-based, wireless, network behavior analysis software, and host-based. The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software. It focuses on enterprise IDPS solutions, but most of the information in the publication is also applicable to standalone and small-scale IDPS deployments.

- **Special Publication 800-95: *Guide to Secure Web Services*** helps organizations understand the challenges in integrating information security practices into Service Oriented Architecture (SOA) design and development based on Web services. It also provides practical, real-world guidance on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services. It also discusses how to make Web services and portal applications robust against the attacks to which they are subject.

- **Special Publication 800-97: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*** helps organizations understand, select, and implement technologies based on Institute of Electrical and Electronics Engineers (IEEE) 802.11i, part of the IEEE 802.11 family of wireless networking standards. The document explains at length the security features and capabilities associated with IEEE 802.11i through its framework for Robust Security Networks (RSN) and provides extensive guidance on planning and deploying RSNs. The document also discusses previous IEEE 802.11 security measures and their shortcomings.

- **Special Publication 800-100: *Information Security Handbook: A Guide for Managers*** provides a broad overview of information security program elements to help managers understand how to establish and implement an information security program.

- **Special Publication 800-111: *Guide to Storage Encryption Technologies for End User Devices*** helps organizations understand storage encryption technologies for end-user devices and for planning, implementing, and maintaining storage encryption solutions. The types of end user devices addressed in this document are personal computers (desktops and laptops), consumer devices (e.g., personal digital assistants, smart phones), and removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs and DVDs). This document provides practical, real-world guidance for three classes of storage encryption techniques: full disk encryption, volume and virtual disk encryption, and file/folder encryption. It also discusses important security elements of a storage encryption deployment, including

cryptographic key management and authentication. It only discusses the encryption of data at rest (storage) and does not address the encryption of data in motion (transmission).

- **Special Publication 800-113: *Guide to SSL VPNs*** helps organizations understand SSL VPN technologies and designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. This document provides a phased approach to SSL VPN planning and implementation that can help achieve successful SSL VPN deployments. It also provides a comparison with other similar technologies, such as IPsec VPNs and other VPN solutions.
- **Special Publication 800-114 Revision 1: *User's Guide to telework and Bring Your Own Device (BYOD) Security*** helps teleworkers secure the networks and BYOD devices they use for telework, such as personally-owned desktop and laptop computers and mobile devices (e.g., smartphones, tablets). This publication focuses specifically on security for telework involving remote access to organizations' non-public computing resources. It provides practical, real-world recommendations for securing telework computers' operating systems (OS) and applications, as well as home networks that the computers use. It presents basic recommendations for securing mobile devices used for telework. This publication also presents advice on protecting the information stored on telework computers and removable media.
- **Special Publication 800-115: *Technical Guide to Information Security Testing and Assessment*** provides guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining technical information relating to security testing and assessment processes and procedures, which can be used for several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements. This guide is not intended to present a comprehensive information security testing or assessment program, but rather an overview of the key elements of technical security testing and assessment with emphasis on specific techniques, their benefits and limitations, and recommendations for their use.
- **Special Publication 800-116 Revision 1: *Guidelines for the Use of PIV Credentials in Facility Access*** provides guidelines on the uses of PIV cards with physical access control systems (PACS). It recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to facilities and assess.
- **Special Publication 800-119: *Guidelines for the Secure Deployment of IPv6*** provides information security guidance to organizations that are planning to deploy IPv6 technologies or are simply seeking a better understanding of IPv6. The scope of this document encompasses the IPv6 protocol and related protocol specifications. IPv6-related security considerations are discussed with emphasis on deployment-related security concerns. The document also includes general guidance on secure IPv6 deployment and integration planning.
- **Special Publication 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*** helps protect the confidentiality of a specific category of data commonly

known as personally identifiable information (PII). PII should be protected from inappropriate access, use, and disclosure. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII. Organizations are encouraged to tailor the recommendations to meet their specific requirements.

- **Special Publication 800-123: *Guide to General Server Security*** helps organizations understand the fundamental activities performed as part of securing and maintaining the security of servers that provide services over network communications as a main function. The types of servers this publication addresses include outward-facing publicly accessible servers, such as web and email services, and a wide range of inward-facing servers. This document discusses the need to secure servers and provides recommendations for selecting, implementing, and maintaining the necessary security controls.

- **Special Publication 800-124 Revision 1: *Guidelines for Managing the Security of Mobile Devices in the Enterprise*** helps organizations centrally manage and secure mobile devices, such as smart phones and tablets. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles.

- **Special Publication 800-125: *Guide to Security for Full Virtualization Technologies*** discusses the security concerns associated with full virtualization technologies for server and desktop virtualization, and provides recommendations for addressing these concerns. All forms of virtualization other than server and desktop full virtualization are outside the scope of this document. Most existing recommended security practices remain applicable in virtual environments. The practices described in this document build on and assume the implementation of practices described in other NIST publications.

- **Special Publication 800-128: *Guide for Security Configuration Management of Information Systems*** elaborates on the application of the Configuration Management family of controls from NIST SP 800-53 (CM-1 through CM-9) and provides guidelines for managing the configuration of the information system architecture and associated components for secure processing, storing, and transmission of information in the information environment. Security configuration management provides an important function for establishing and maintaining secure information system configurations and provides important support for managing risks in information systems.

- **Special Publication 800-137: *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*** helps organizations develop an Information Security Continuous Monitoring (ISCM) strategy and implement an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effective deployment of security controls. The ISCM strategy and program support ongoing assurance

that planned and implemented security controls are aligned with organizational risk tolerance, as well as the information needed to respond to risk in a timely manner.

- **Special Publication 800-144: *Guidelines on Security and Privacy in Public Cloud Computing*** provides an overview of public cloud computing and the security and privacy challenges involved. The document discusses the threats, technology risks, and safeguards for public cloud environments, and provides the insight needed to make informed information technology decisions on their treatment. The document does not prescribe or recommend any specific cloud computing service, service arrangement, service agreement, service provider, or deployment model. Each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the public cloud services that can best fulfill those needs.
- **Special Publication 800-145: *The NIST Definition of Cloud Computing*** characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what cloud computing is to how best to use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.
- **Special Publication 800-146: *Cloud Computing Synopsis and Recommendations*** explains the cloud computing technology area in plain terms and provides recommendations for information technology decision makers.
- **Special Publication 800-147: *BIOS Protection Guidelines*** provides guidelines for preventing the unauthorized modification of Basic Input/Output System (BIOS) firmware on PC client systems. It also provides platform vendors with recommendations and guidelines for a secure BIOS update process.
- **Special Publication 800-150: *Guide to Cyber Threat Information Sharing*** provides guidance to help organizations exchange cyber threat information. The guidance addresses sharing cyber threat information within an organization, consuming and using cyber threat information received from external sources, and producing cyber threat information that can be shared with other organizations. The document also presents specific considerations for participation in information sharing communities. This publication expands upon the information sharing concepts introduced in Section 4, Coordination and Information Sharing, of NIST Special Publication (SP) 800-61.
- **Special Publication 800-153: *Guidelines for Securing Wireless Local Area Networks (WLAN s)*** provides organizations with recommendations for improving the security configuration and monitoring of their IEEE 802.11 wireless local area networks (WLANs) and their devices connecting to those networks. The scope of this publication is limited to unclassified wireless networks and unclassified facilities within range of unclassified wireless networks.

Conclusion

Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs and the success of the resulting security measures employed to protect the information and information systems. The implementation of information security controls is vital to protecting an agency's information as well as its reputation, legal position, personnel, and other tangible or intangible assets. Well-developed security rules and procedures that are in place to protect important information support the agency's overall mission. In today's environment of malicious code, system breaches, and insider threats, publicized security issues can have dire consequences, especially to the service of customers.

Thus, SWAs need to develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in FIPS Publication 200 and ensure their effective implementation.

ETA strongly recommends that SWAs use FIPS 199 for system categorization, FIPS 200/NIST SP 800-53 for the specification of the security controls, and NIST SP 800-53A for the assessment of security control effectiveness.