NIST Special Publication 800-175A

Guideline for Using Cryptographic Standards in the Federal Government:

Directives, Mandates and Policies

Elaine Barker
William C. Barker

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-175A

C O M P U T E R S E C U R I T Y

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-175A

Guideline for Using Cryptographic Standards in the Federal Government:

Directives, Mandates and Policies

Elaine Barker
Computer Security Division
Information Technology Laboratory

William C. Barker
Domestic Guest Researcher
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-175A

August 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-175A
Natl. Inst. Stand. Technol. Spec. Publ. 800-175A, 37 pages (August 2016)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-175A

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: SP800-175@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document is part of a series intended to provide guidance to the Federal Government for using cryptography and NIST's cryptographic standards to protect sensitive, but unclassified digitized information during transmission and while in storage. Special Publication (SP) 800-175A provides guidance on the determination of requirements for using cryptography. It includes a summary of laws and regulations concerning the protection of the Federal Government's sensitive information, guidance regarding the conduct of risk assessments to determine what needs to be protected and how best to protect that information, and a discussion of the relevant security-related documents (e.g., various policy and practice documents).

Keywords

authentication; confidentiality; critical infrastructure; cryptographic guideline; cryptography; Executive Orders; integrity; key management; laws; mandates; policy; Presidential Directives; risk assessment; standards.

Acknowledgments

The authors wish to thank the authors of NIST Special Publication (SP) 800-21 from which this document was derived, including Annabelle Lee, along with those colleagues that reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Table of Contents

SECTION 1: INTRODUCTION 1
1.1 Background and Purpose 1
1.2 Terms and Definitions 1
1.3 Acronyms 5
1.4 Document Organization 6
SECTION 2: APPLICABLE PUBLIC LAWS 7
2.1 E-Government Act of 2002 (FISMA) 7
2.2 Health Information Technology for Economic and Clinical Health (HITECH) Act 9
2.3 Federal Information Systems Modernization Act of 2014 9
2.4 Cybersecurity Enhancement Act of 2014 10
SECTION 3: EXECUTIVE DIRECTION 12
3.1 Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection 12
3.2 HSPD-12: Policies for a Common Identification Standard for Federal Employees and Contractors 12
3.3 Executive Order 13636: Improving Critical Infrastructure Cybersecurity 13
3.4 OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities 14
3.5 OMB Circular A-130: Managing Information as a Strategic Resource 14
3.6 OMB Memorandum M-06-16: Protection of Sensitive Agency Information 23
3.7 OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12 24
3.8 OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information 24
3.9 OMB Memorandum M-08-23: Securing the Federal Government's Domain Name System Infrastructure (DNS) 25
3.10 OMB Memorandum M-11-33: FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management 26
3.11 OMB Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements 28
SECTION 4: ORGANIZATIONAL POLICIES 29
4.1 Information Management Policy 29
4.2 Information Security Policy 29
4.3 Key Management Policies 29
SECTION 5: RISK MANAGEMENT PROCESS 31

5.1 Categorization of Information and Information Systems 32
5.2 Selection of Security Controls 32
APPENDIX A: REFERENCES 33

SECTION 1: INTRODUCTION

1.1 Background and Purpose

Cryptographic publications of the National Institute of Standards and Technology (NIST) provide guidance regarding how cryptographic protection is to be implemented, but do not specify when cryptographic protection is required. The decision regarding whether or not to employ cryptographic protection rests with the owner of the information to be protected. Decisions concerning the use of cryptographic protection are generally based on a thorough risk analysis that establishes the sensitivity of the information to be protected and the security controls that need to be used to protect that information, both during transmission and while in storage. This document provides guidance on the basis for determining requirements for using cryptography. It includes a summary of the laws, directives, standards, and guidelines concerning the protection of the Federal government's sensitive but unclassified information; guidance regarding the conduct of risk assessments to determine what information needs to be protected and how best to protect that information; and a discussion of application-relevant security documentation (e.g., various policy and practice documents). While the use of this guideline outside the Federal Government is strictly voluntary, many of the processes and references included herein may be useful in non-federal contexts.

The primary policy documents that apply to federal cryptographic systems include Public Laws, Presidential Executive Orders and Directives, and other guidance from Executive Office of the President organizations. Some Department of Commerce and NIST publications are identified in these policy documents as being mandatory for Federal organizations. Relevant NIST cryptographic publications are discussed in Special Publication (SP) 800-175B, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.*

1.2 Terms and Definitions

Authentication	As used in this document, a process that provides assurance of the source and integrity of information that is communicated or stored, or that provides assurance of an entity's identity.
Authorization	The official management decision given by a senior organizational official to authorize the operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or where authorized users take actions for an other than authorized purposes, have access or potential

	access to sensitive information, whether physical or electronic.
Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems.
Ciphertext	Data in its encrypted form.
Confidentiality	The property that sensitive information is not disclosed to unauthorized entities.
Critical Infrastructure	The essential services that support a society and serve as the backbone for the society's economy, security and health.
Cryptographic algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key (if applicable), and produces an output.
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.
Cryptography	The science of information hiding and verification. It includes the protocols, algorithms and methodologies to securely and consistently prevent unauthorized access to sensitive information and enable verifiability of the information. The main goals include confidentiality, integrity authentication and source authentication.
Digital Infrastructure	The Digital Infrastructure is defined as the ability to store and exchange data through a centralized communication system. Data communication and exchange are all simplified with the right software and hardware equipment.
Encryption	The process of transforming plaintext into ciphertext for the purpose of security or privacy.
Entity	An individual (person), organization, device or process.
Executive Office of the President	The President's immediate staff, along with entities such as the Office of Management and Budget, the National Security Staff, the Office of Science and Technology Policy, and the Office of Personnel Management.
Executive Orders	Legally binding orders given by the President, acting as the head of the Executive Branch, to Federal Administrative Agencies. Executive Orders are generally used to direct

	federal agencies and officials in their execution of congressionally established laws or policies.
High Impact	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.
Identity Management	Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users.
Integrity	The property that protected data has not been modified or deleted in an unauthorized and undetected manner.
Key Establishment	The procedure that results in keying material that is shared among different parties.
Keying Material	The data (e.g., keys) necessary to establish and maintain cryptographic keying relationships.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., counters) during the entire life cycle of the keys, including the generation, storage, establishment, entry and output, and destruction.
Low-Impact	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Mandate	A mandatory order or requirement under statute.
Moderate Impact	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Plaintext	Intelligible data that has meaning and can be understood without the application of cryptography.
Policy	The set of basic principles and associated guidelines, formulated and enforced by the governing body of an organization, to direct and limit its actions in pursuit of long-term goals.
Presidential Directive	A form of an executive order issued by the President of the United States with the advice and consent of the National Security Council; also known as a Presidential Decision Directive (or PDD).

Reciprocity	The mutual agreement among participating organizations to accept each other's security assessments in order to reuse information-system resources and/or to accept each other's assessed security posture in order to share information.
Risk Analysis	See risk assessment.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, images, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, images, and reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Policy	A set of criteria for the provision of security services.
Security Strength	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system.
Standard	A document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.
Two-Factor Authentication	Proof of the possession of a physical or software token in combination with some memorized secret knowledge.

1.3 Acronyms

CIO	Chief Information Officer
CNSS	Committee for National Security Systems
DHS	Department of Homeland Security
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
EOP	Executive Office of the President
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act (P.L. 107-347)
GSA	General Services Administration
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
IG	Inspector General
IT	Information Technology
ITL	Information Technology Laboratory
JTFTI	Joint Task Force Transformation Initiative
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NPIVP	NIST Personal Identity Verification Program
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PHI	Protected Health Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
P.L.	Public Law
SAOP	Senior Agency Official for Privacy
SP	Special Publication

U.S.C. United States Code

1.4 Document Organization

This publication is organized as follows:

- Section 1 provides an introduction to this document, including its background and purpose, a definition of terms, and a list of acronyms used herein.
- Section 2 describes legislative mandates that are relevant to the cryptographic standards and guidelines that are developed by NIST, or in the development of which NIST participates.
- Section 3 discusses directives from the Executive Office of the President (EOP) that are relevant to cryptographic standards and guidelines that are developed by NIST, or in the development of which NIST participates.
- Section 4 provides a brief treatment of organization-specific policies that may prescribe the cryptographic services that need to be provided and the level of protection needed.
- Section 5 provides a brief treatment of the risk management process that determines security control requirements – including cryptographic requirements.
- Appendix A includes a list of references.

SECTION 2: APPLICABLE PUBLIC LAWS

This section describes elements of legislative mandates that are relevant to the cryptographic standards and guidelines that are developed by NIST, or in the development of which NIST participates.

2.1 E-Government Act of 2002 (FISMA)

Title III of Public Law 107-347 is cited as the Federal Information Security Management Act of 2002 (FISMA) and has been incorporated into Sections 20 and 21 of the NIST Act.

Paragraph 3543 of the Act provides for the Executive Office of the President to coordinate the development of standards and guidelines by the National Institute of Standards and Technology (NIST) (under Section 20 of the National Institute of Standards and Technology Act [15 U.S.C. 278g–3]) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems.

Section 302 of the Act directs the Secretary of Commerce (under Section 11331 of Title 40 United States Code (U.S.C.)) to prescribe standards and guidelines pertaining to federal information systems, based on standards and guidelines developed by NIST. Section 302 of the Act makes these standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of the operation or security of federal information systems, and also states that the standards shall include information security standards that—

(1) Provide minimum information security requirements as determined under Section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

(2) Are otherwise necessary to improve the security of federal information and information systems.

Only the President is assigned the authority to disapprove or modify these standards.

The heads of executive agencies may employ standards for the cost-effective information security of information systems within or under the supervision of that agency that are more stringent than the standards prescribed by the Secretary of Commerce if the more stringent standards — (1) contain at least the applicable standards made compulsory and binding by the Secretary; and (2) are otherwise consistent with policies and guidelines issued under Section 3543 of Title 44 U.S.C. Section 302 also requires that the Secretary of Commerce promulgate any standard under the section not later than six months after the submission of the proposed standard to the Secretary by NIST, as provided under Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

Section 303 of the Act amends Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), to require NIST to:

(1) Have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

(2) Develop standards and guidelines, including minimum requirements, for information systems other than national security systems (as defined in Section 3542(b)(2) of Title 44,

United States Code) that are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in Section 3542(b)(2) of Title 44, United States Code); and

(3) Develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; such standards and guidelines do not apply to national security systems.

Section 303 requires the standards and guidelines to include, among other things:

(1) Standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency, based on the objectives of providing appropriate levels of information security according to a range of risk levels;

(2) Guidelines recommending the types of information and information systems to be included in each such category;

(3) Minimum information-security requirements for information and information systems in each category; and

(4) A definition of and guidelines concerning the detection and handling of information-security incidents.

To the maximum extent practicable, NIST is required, by Section 303 of the Act, to:

(1) Ensure that its security standards and guidelines do not require the use or procurement of specific products, including any specific hardware or software;

(2) Ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information-security risks; and

(3) Use flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information-security products.

Among other requirements of Section 303 of the Act, NIST is required to:

(1) Submit standards developed to the Secretary of Commerce for promulgation under Section 11331 of Title 40, United States Code, along with recommendations as to the extent to which these standards should be made compulsory and binding;

(2) Provide technical assistance to agencies, upon request, regarding complying with the standards and guidelines, detecting and handling information-security incidents, and information-security policies, procedures, and practices;

(3) Conduct research, as needed, to determine the nature and extent of information-security vulnerabilities and techniques for providing cost-effective information security;

(4) Develop and periodically revise performance indicators and measures for agency information-security policies and practices;

(5) Evaluate private-sector information-security policies and practices and commercially available information technologies to assess the potential application by agencies to strengthen information security;

(6) Assist the private sector, upon request, in using and applying the results of activities under this section;

(7) Evaluate security policies and practices developed for national security systems to assess the potential for application by agencies to strengthen information security; and

(8) Periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions, as appropriate.

2.2 Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 is an example of sector-specific legislation that provides for the encryption of information using NIST standards. The HITECH Act was enacted, as Title XIII of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the rules enacted by the Health Insurance Portability and Accountability Act (HIPAA) of 1996[1]. The HITECH Act mandates the notification of a breach of unsecured protected health information (PHI), but provided that breaches do not have to be reported if the data involved is rendered unreadable via encryption[2].

2.3 Federal Information Systems Modernization Act of 2014

The Federal Information Systems Modernization Act of 2014 moves some of the Office of Management and Budget (OMB) responsibilities mandated by the Federal Information Security Management Act of 2002 from the Director of the Office of Management and Budget to the Secretary for Homeland Security. Paragraph 3553 requires the Secretary for Homeland Security to:

(1) Coordinate the development of standards and guidelines by NIST (under Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3)) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

[1] https://www.gpo.gov/fdsys/pkg/PLAW-104publ191.

[2] Data encryption, however, must be validated for compliance with NIST Federal Information Processing Standard (FIPS) 140-2, according to the Interim Final Rule that further spelled out breach notification requirements. This HHS guidance is also to be used to render identifiable health information unusable, unreadable, or indecipherable for purposes of the temporary breach notification requirements that apply to vendors of Personal Health Records (PHRs), the requirements for which are to be administered by the Federal Trade Commission (which in turn issued proposed regulations on April 16, 2009, addressing consumer notices for breaches of electronic health information by PHRs). The HHS guidance provides two methods of securing information for the purposes of the HITECH Act: destruction and encryption. Destruction may secure information that was found in either paper form or in electronic media. In order to satisfy the destruction method, the paper or other hard-copy media must be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Electronic media must be cleared, purged, or destroyed in accordance with the specifications set forth in NIST SP 800-88. (See 74 Fed. Reg. at 19010.)

(2) Coordinate Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council (established under Section 3603 of the Act) and the Director of NIST;

(3) Develop and oversee the implementation of binding operational directives for agencies to implement the policies, principles, standards, and guidelines developed by the Department of Homeland Security (DHS), and consider any applicable standards or guidelines developed by NIST and issued by the Secretary of Commerce under Section 11331 of Title 40;

(4) Consult with the Director of NIST regarding any binding operational directive issued by DHS that implements standards and guidelines developed by NIST; and

(5) Ensure that the binding operational directives do not conflict with the standards and guidelines issued under Section 11331 of Title 40.

Paragraph 3553 of the Act also provides that nothing in the subchapter is to be construed as authorizing the Secretary for Homeland Security to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under Section 11331 of Title 40; and that nothing in this subchapter, (Section 11331 of Title 40), or Section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including information related to the protection of personal privacy under Title 5 or Title 44 U.S.C.

2.4 Cybersecurity Enhancement Act of 2014

The Cybersecurity Enhancement Act of 2014 extends NIST's security standards activity to include direct support to the private sector. The security standards' responsibility extension includes cryptographic standards. This extension is significant in that it specifically authorizes cybersecurity support for organizations outside the U.S. Federal government.

Specifically, the Act's *Title I: Public-Private Collaboration on Cybersecurity* - (Sec. 101) amends the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of NIST, to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to a critical infrastructure. The Act requires the NIST Director, in carrying out such activities, to:

(1) Coordinate regularly with, and incorporate the industry expertise of, relevant private-sector personnel and entities, critical infrastructure owners and operators, sector-coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations;

(2) Consult with the heads of agencies with national security responsibilities, sector-specific agencies, state and local governments, governments of other nations, and international organizations;

(3) Identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information-security measures and controls, that may be voluntarily

adopted by owners and operators of a critical infrastructure to help identify, assess, and manage cyber risks; and

(4) Include methodologies to mitigate impacts on business confidentiality, protect individual privacy and civil liberties, incorporate voluntary consensus standards and industry best practices, align with international standards, and prevent duplication of regulatory processes.

However, the Act prohibits the Director from prescribing a specific solution or requiring that products or services be designed or manufactured in a particular manner, and it prohibits information provided to NIST for purposes of developing cyber-risk standards from being used by federal, state, tribal, or local agencies to regulate the activity of any entity.

The Act's Title II: Cybersecurity Research and Development - (Sec. 201) directs agencies to build upon existing programs to meet cybersecurity objectives, such as how to:

(1) Guarantee individual privacy, verify third-party software and hardware, and address insider threats;

(2) Determine the origin of messages transmitted over the Internet; and

(3) Protect information stored using cloud computing or transmitted through wireless services.

Title II also requires agencies to describe how they will focus on technologies to protect consumer privacy and enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure.

The Act's Title V: Advancement of Cybersecurity Technical Standards - (Sec. 502) requires NIST to ensure the coordination of federal agencies engaged in the development of international technical standards related to information system security and instructs NIST to ensure consultation with appropriate private-sector stakeholders.

Section 503 of the Act requires consideration to be given to activities that support (in consultation with the private sector) the development of appropriate security frameworks and reference materials, and the identification of best practices, for federal agencies to use in addressing security and privacy requirements.

Section 504 of the Act requires NIST to continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria with regard to identity management research and development.

SECTION 3: EXECUTIVE DIRECTION

This section describes directives from the Executive Office of the President (EOP) that are relevant to cryptographic standards and guidelines that are developed by NIST, or in the development of which NIST participates.

3.1 Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection

HSPD-7 establishes a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. The Directive directs the Department of Commerce, in coordination with the Department for Homeland Security, to work with the private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act[3] to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

3.2 HSPD-12: Policies for a Common Identification Standard for Federal Employees and Contractors

This directive mandates the development of a federal standard for secure and reliable forms of identification. HSPD-12 directs the Secretary of Commerce to promulgate, in accordance with applicable laws, a federal standard for secure and reliable forms of identification in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce is directed to periodically review the Standard and update the Standard, as appropriate, in consultation with the affected agencies. For purposes of this directive, "Secure and reliable forms of identification" means identification that:

(a) Is issued, based on sound criteria for verifying an individual employee's identity;

(b) Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

(c) Can be rapidly authenticated electronically; and

(d) Is issued only by providers whose reliability has been established by an official accreditation process.

The Standard to be developed is directed to include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

[3] https://www.fema.gov/media-library-data/1438002689366-c84ffcf6e8476f44e0921a70a4556f88/Defense_Production_Act_2014.pdf

3.3 Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Section 7 of Executive Order 13636, titled "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure," requires the Secretary of Commerce to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructures (the *Cybersecurity Framework*). The *Cybersecurity Framework* was required to:

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;
- Incorporate voluntary consensus standards and industry best practices to the fullest extent possible;
- Be consistent with voluntary international standards when such international standards will advance the objectives of this order; and
- Meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

The *Cybersecurity Framework* was required to:

- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls;
- Help owners and operators of critical infrastructures identify, assess, and manage cyber risk;
- Focus on identifying cross-sector security standards and guidelines applicable to the critical infrastructure;
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations;
- In order to enable technical innovation and account for organizational differences, to provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks; and
- Include guidance for measuring the performance of an entity in implementing the *Cybersecurity Framework*.

The *Cybersecurity Framework* was also required to include methodologies to identify and mitigate impacts of the *Cybersecurity Framework* and associated information-security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

In developing the *Cybersecurity Framework*, NIST was directed to engage in an open public review and comment process. The Director is also required to consult with the Secretary for Homeland Security, the National Security Agency, Sector-Specific agencies and other interested agencies, including OMB, owners and operators of critical infrastructure, and other stakeholders.

3.4 OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities

OMB Circular A-119 establishes policies on the Federal use and development of voluntary consensus standards and on conformity assessment activities. Public Law 104-113, the "National Technology Transfer and Advancement Act of 1995," codified existing policies in A-119, established reporting requirements, and authorized the National Institute of Standards and Technology to coordinate conformity assessment activities of the agencies. OMB is issuing this revision of the Circular in order to:

- Make the terminology of the Circular consistent with the National Technology Transfer and Advancement Act of 1995,
- Issue guidance to the agencies on making their reports to OMB,
- Direct the Secretary of Commerce to issue policy guidance for conformity assessment, and
- Make changes for clarity.

3.5 OMB Circular A-130: Managing Information as a Strategic Resource

Office of Management and Budget Circular A-130[4] establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. The appendices to this Circular also include responsibilities for protecting Federal information resources and managing personally identifiable information (PII). The requirements of this Circular apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government. The requirements of Circular A-130 apply to management activities concerning all information resources in any medium (unless otherwise noted), including paper and electronic information. When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements of this Circular is not shifted (to the service provider). Agencies are required to describe the responsibilities of service providers in relevant agreements with the service providers. Agencies are not required to apply this Circular to national security systems (defined in 44 U.S.C. § 3552[5]), but are encouraged to do so where appropriate. For national security systems, agencies shall follow applicable statutes, executive orders, directives, and internal agency policies.

Unlike most other cybersecurity-related directives and mandates, Circular A-130 does impose specific requirements for encryption and digital signatures. The following material identifies particularly salient requirements associated with cryptography and the underlying risk management determinations. Within each subsection below, paragraph numbers associated with lists are preserved from the Circular in order to facilitate reference.

[4] Although this Circular touches on many specific information resources management issues such as privacy, confidentiality, information quality, dissemination, and statistical policy, those topics are covered more fully in other Office of Management and Budget (OMB) policies, which are available on the OMB website. Agencies shall implement the policies in this Circular and those in other OMB policy guidance in a mutually consistent fashion.
[5] https://www.gpo.gov/fdsys/pkg/USCODE-2014-title44/html/USCODE-2014-title44-chap35-subchapII-sec3552.htm

3.5.1 Privacy And Information Security Provisions

Section 5, "Policy," subparagraph f, "Privacy and Information Security," subparagraph 2), "Information Security," requires agencies to provide proper safeguards to:

a) Ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014;

b) Protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information; and

c) Implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs).[6]

3.5.2 Electronic Signature Provisions

Section 5, "Policy," subparagraph g, "Electronic Signatures," subparagraph 3), "Information Security," requires agencies to:

1) Allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and for agencies to maintain records electronically, when practicable. Electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form;

2) Promote the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between: contracts written on paper and contracts in electronic form; pen-and-ink signatures and electronic signatures; and other legally required written documents (termed "records") and the same information in electronic form; and

3) Develop and implement processes to support use of digital signatures, a form of electronic signature, for employees and contractors.

3.5.3 Government-wide Responsibilities

The following provisions are directed by Section 6, "Government-wide Responsibilities."

[6] NISTIRs describe research of a technical nature of interest to a specialized audience; NIST's cybersecurity NISTIRs are available at http://csrc.nist.gov/publications/PubsNISTIRs.html.

a. Department of Commerce

The Secretary of Commerce shall:

1) Develop and issue standards and guidelines for the security and privacy of information in Federal information systems and systems which create, collect, Federal Government; process, store, transmit, disseminate, or dispose of information on behalf of the Federal Government; [7]

2) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of IT;[8]

3) Conduct studies and evaluations concerning telecommunications technology, and the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;

4) Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting Federal information activities;

5) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;[9]

6) Ensure that the Federal Government is represented in the development of national and international (in consultation with the Secretary of State) IT standards, and advise the Director of OMB on such activities;[10]

7) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense (DOD) and DHS;

9) Lead the development of a Cybersecurity Framework to reduce cyber risks to critical infrastructure pursuant to Executive Order 13636, Improving Critical Infrastructure Cybersecurity.

3.5.4 General Requirements for Protecting and Managing Federal Information Resources

Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources," under Section 3, "General Requirements," directs that:

[7] National Institute of Standards and Technologies (NIST) Act, 15 U.S.C. § 278g-3.

[8] Pursuant to the NIST Act (15 U.S.C. § 278g-3).

[9] Pursuant to the NIST Act, 15 U.S.C. §§ 272(b), 278g-3, and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

[10] Pursuant to NIST Act, 15 U.S.C. §§ 272(b), 273, 278g–3 and OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.

a. Agencies shall implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security and privacy risk on an ongoing basis across the three organizational tiers (i.e., organization level, mission or business process level, and information system level).[11]

b. [Omitted from this publication as being out of scope.]

c. Agencies that share PII shall require, as appropriate, other agencies and entities with which they share PII to maintain the PII in an information system with a particular NIST FIPS Publication 199 confidentiality impact level, as determined by the agency sharing the PII.

d. Agencies that share PII with other agencies or entities shall impose, where appropriate, conditions (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII through written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding.

e. Agencies shall protect Controlled Unclassified Information (CUI) and shall apply NIST FIPS and NIST (800-series) SPs[12], as appropriate. This includes limiting the disclosure of proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists.

f. Agencies shall ensure compliance with all applicable statutory, regulatory, and policy requirements and develop and maintain effective information security and privacy programs. This includes using privacy impact assessments and other tools to manage privacy risks.

g. Agencies shall implement policies issued by OMB, as well as requirements issued by the Department of Commerce, DHS, GSA, and OPM. This includes applying the standards and guidelines contained in NIST FIPS, NIST (800-series) SPs, and, where appropriate and directed by OMB, NISTIRs.

3.5.5 Specific Requirements for Protecting and Managing Federal Information Resources

Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources," under Section 4, "Specific Requirements," directs:

a. Security Categorization

[11] NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, provides additional information on risk management processes and strategies.
[12] NIST's FIPS and SP 800-series publications are available at http://csrc.nist.gov/publications/PubsFIPS.html and http://csrc.nist.gov/publications/PubsSPs.html, respectively.

Agencies shall:

1) Identify authorization boundaries for information systems in accordance with NIST SPs 800-18 and 800-37; and

2) Categorize information and information systems, in accordance with FIPS Publication 199 and NIST SP 800-60, considering potential adverse security and privacy impacts to organizational operations and assets, individuals, other organizations, and the Nation.

c. Plans, Controls, and Assessments

Agencies shall:

5) Employ a process to select and implement security controls for information systems and the environments in which those systems operate[13] that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST SP 800-53, tailored as appropriate;

6) Employ a process to select and implement privacy controls for information systems and programs that satisfies applicable privacy requirements in OMB guidance, including, but not limited to, Appendix I to this Circular and OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act;

7) Implement information system security using sound systems security engineering principles, concepts, methods, practices, and techniques;

8) Develop and maintain security plans for information systems to document which security controls have been selected and how those controls have been implemented that satisfies the minimum information security requirements in FIPS Publication 200 and security control baselines in NIST SP 800-53, tailored as appropriate.[14]

10) Deploy effective security controls to provide Federal employees and contractors with multifactor authentication, digital signature, and encryption capabilities that provide assurance of identity and are interoperable Government-wide and accepted across all Executive Branch agencies;

[13] The environment of operation includes the physical surroundings in which an information system processes, stores, and transmits information. Agencies should take the environment into account when selecting, implementing, documenting, and assessing security controls.

[14] Agencies must conduct tailoring activities in accordance with OMB policy.

11) Adhere to Government-wide requirements in the deployment and use of identity credentials used by employees and contractors accessing Federal facilities;[15]

12) Designate common controls in order to provide cost-effective security and privacy[16] capabilities that can be inherited by multiple agency information systems or programs;

13) Conduct and document assessments of all selected and implemented security and privacy controls to determine whether security and privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable requirements and to manage security and privacy risks;

14) Conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance.

i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems[17]

Agencies shall:

4) Isolate sensitive or critical information resources (e.g., information systems, system components, applications, databases, and information) into separate security domains with appropriate levels of protection based on the sensitivity or criticality of those resources;

8) Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement;[18]

[15] NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, provides additional information on the use of PIV Credentials, the Government-wide standard identity credential, in physical access control systems. Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.

[16] When common controls protect multiple agency information systems of differing impact levels, the controls shall be implemented at the highest impact level among the systems. If such controls cannot be implemented at the highest impact level of the information systems, agencies shall factor this situation into their assessments of risk and take appropriate risk mitigation actions (e.g., adding security controls, changing assigned values of security control parameters, implementing compensating controls, changing certain aspects of mission or business processes, or separating the higher impact system into its own domain where it can be afforded appropriate levels of protection).

[17] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides information on additional security safeguarding measures.

11) Require use of multifactor authentication for employees and contractors in accordance with Government-wide identity management standards;[19]

12) Develop and implement processes to support use of digital signatures for employees and contractors;

13) Ensure that all public key infrastructure (PKI) certificates used by an agency and issued in accordance with Federal PKI policy validate to the Federal PKI trust anchor when being used for user signing, encrypting purposes, authentication and authorization;[20]

14) Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate);[21]

15) Implement the current encryption algorithms and validated cryptographic modules in accordance with NIST standards and guidelines;

16) Ensure that only individuals or processes acting on behalf of individuals with legitimate need for access have the ability to decrypt sensitive information;

17) Implement data-level protection and access controls to ensure the security of and access to Federal information; and

[18] Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides additional guidance on unsupported software components.

[19] Pursuant to Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, NIST FIPS 201 describes the initial Government-wide identity management standard for employees and contractors as a smartcard form factor (the PIV card). With the emergence of a newer generation of computing devices and in particular with mobile devices, the use of PIV cards has evolved technically to include other form factors that can be deployed directly with mobile devices as specified in NIST SP 800-157. The PIV credential associated with this alternative is called a Derived PIV Credential. Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63. Issuing a Derived PIV credential to PIV card holders does not require repeating identity proofing and vetting processes. The user simply proves possession and control of a valid PIV Card to receive a Derived PIV Credential.

[20] The trust anchor refers to the Federal PKI root certificate operated by the Federal PKI Management Authority. This root certificate is the trusted source of all Federal PKI certificates. For additional information, refer to https://www.idmanagement.gov and Federal PKI policy.

[21] The encryption of organizational information when in transit over a network and when at rest in storage devices ensures that such information is persistently protected and promotes a defense-in-depth security strategy.

18) Ensure that all Federal systems and services identified in the Domain Name System are protected with Domain Name System Security (DNSSEC) and that all systems are capable of validating DNSSEC protected information.[22]

m. Encryption

When the assessed risk indicates the need, agencies must encrypt Federal information at rest and in transit unless otherwise protected by alternative physical and logical safeguards implemented at multiple layers, including networks, systems, applications, and data. Encrypting information at rest and in transit helps to protect the confidentiality and integrity of such information by making it less susceptible to unauthorized disclosure or modification. Agencies must apply encryption requirements to Federal information categorized as either moderate or high impact in accordance with FIPS Publication 199 unless encrypting such information is technically unfeasible or would demonstrably affect their ability to carry out their respective mission, functions, or operations. In situations where the use of encryption is technically infeasible, for example, due to an aging legacy system, agencies must initiate the appropriate system or system component upgrade or replacement actions at the earliest opportunity to be able to accommodate such safeguarding technologies. Authorizing officials who choose to operate information systems without the use of required encryption technologies must carefully assess the risk in doing so, and they must receive written approval for the exception from the agency CIO, in consultation with the SAOP (as appropriate). Only FIPS-validated cryptography is approved for use in Federal information systems covered by this policy.

n. Digital Signatures

Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use. Additionally, digital signatures can help agencies streamline mission or business processes and transition manual processes to more automated processes to include, for example, online transactions. Because of the advantages provided by this technology, OMB expects agencies to implement digital signature capabilities in accordance with Federal PKI policy, and NIST standards and guidelines. For employees and contractors, agencies must require the use of the digital signature capability of Personal Identity Verification (PIV) credentials. For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures.

3.5.6 NIST Documents Cited By Circular A-130

Circular A-130 cites the following NIST documents as references:

[22] DNSSEC is a critical component of the Internet infrastructure. DNSSEC enables clients to cryptographically verify that each such translation is provided by a server with the authority to do so, and that the translation response from the server was not modified before reaching the client.

8) National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

9) National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

10) National Institute of Standards and Technology Federal Information Processing Standards Publication 201, Personal Identity Verification of Federal Employees and Contractors.

11) National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems.

12) National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments.

13) National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

14) National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

15) National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems.

16) National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

17) National Institute of Standards and Technology Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.

18) National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.

19) National Institute of Standards and Technology Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

20) National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline.

21) National Institute of Standards and Technology Special Publication 800-73, Interfaces for Personal Identity Verification.

22) National Institute of Standards and Technology Special Publication 800-76, Biometric Specifications for Personal Identity Verification.

23) National Institute of Standards and Technology Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.

24) National Institute of Standards and Technology Special Publication 800-79, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).

25) National Institute of Standards and Technology Special Publication 800-116, Guidelines for the Use of PIV Credentials in Physical Access Control Systems (PACS).

26) National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

27) National Institute of Standards and Technology Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

28) National Institute of Standards and Technology Special Publication 800-157, Guidelines for Derived Personal Identity Verification Credentials.

29) National Institute of Standards and Technology Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

30) National Institute of Standards and Technology Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

31) National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

32) National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity.

33) National Institute of Standards and Technology Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management.

3.6 OMB Memorandum M-06-16: Protection of Sensitive Agency Information

OMB Memorandum M-06-16 notes that NIST provided a checklist for the protection of remote information. The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, OMB M-06-16 recommended that all departments and agencies encrypt all data on mobile computers/devices that carry agency data

unless the data is determined to be non-sensitive, in writing, by a Deputy Secretary or an individual that he/she may designate in writing; and allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

3.7 OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12

OMB Memorandum M-06-18 provides updated direction for the acquisition of products and services for the implementation of Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, and also provides the status of implementation efforts.

HSPD-12 notes that both NIST and the General Services Administration (GSA) have established evaluation programs for the testing and evaluation of specific products and services needed for the implementation of HSPD-12, and that NIST has established the NIST Personal Identity Verification Program (NPIVP) to test and validate Personal Identity Verification (PIV) components and sub-systems required by Federal Information Processing Standard (FIPS) 201. At the time that the Memorandum was signed, an NPIVP validation program provided for the testing and validation of PIV card applications and PIV middleware for conformance to FIPS 201 and the interface specifications of NIST SP 800-73, *Interfaces for Personal Identity Verification*. NIST was also noted as having published derived test requirements as NIST SP 800-85A, *PIV Card Application and Middleware Test Guidelines.* All of the tests under NPIVP are handled by third-party test laboratories that are now designated as interim NPIVP Test Facilities.

FIPS 140-2, *Security Requirements for Cryptographic Modules*[23], requires the testing and validation of the cryptographic modules of PIV cards and other products performing cryptographic functions. This testing is performed by the accredited third-party facilities designated to perform NPIVP testing.

3.8 OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

OMB Memorandum M-07-16 requires agencies to develop and implement a breach[24] notification policy within 120 days from the OMB Memorandum's having been signed. The Memorandum specifically recommends using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy, while ensuring that proper safeguards are in place to protect the information. Elements of the framework include requirements to:

[23] Note that implementation of FIPS 140-2 by the Cryptographic Module Validation Program is accomplished in accordance with the *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, which is periodically updated to list additional clarification/guidance relating to FIPS 140-2.

[24] For the purposes of this policy, the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

a. Assign an impact level to all information and information systems. Agencies must follow the processes outlined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (i.e., low, moderate, and high). Agencies should generally consider categorizing sensitive, personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*[25], respectively.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*,[26] and include guidance for the continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

The Memorandum's requirements include 1) encryption using only NIST-certified cryptographic modules[27] for all data on mobile computers/devices carrying agency data, unless the data is determined to not be sensitive, in writing, by a Deputy Secretary[28] or a senior-level individual he/she may designate in writing; and 2) allowing remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

3.9 OMB Memorandum M-08-23: Securing the Federal Government's Domain Name System Infrastructure (DNS)

OMB Memorandum M-08-23 required the Federal Government to deploy Domain Name System Security Extensions (DNSSEC) to the top-level .gov domain by January 2009. The top-level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top-level .gov domain will be DNSSEC-signed, and processes to enable secure delegated sub-domains will be developed. Signing the top-level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower-level deployment by agencies.

The Memorandum also required agencies to develop plans of action and milestones for the deployment of DNSSEC to all applicable information systems. Appropriate DNSSEC capabilities were required to be deployed and operational by December 2009. The plans were to follow recommendations in NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, and

[25] The current Revision 4 of SP 800-53 is titled *Security and Privacy Controls for Federal Information Systems and Organizations*.
[26] Since reissued as SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework for Federal Information Systems: A Security Life Cycle Approach*. Note that certification is no longer required and the term *C&A* is now obsolete.
[27] See NIST's website at http://csrc.nist.gov/cryptval/ for a discussion of the validated encryption modules.
[28] Non-cabinet agencies should consult the equivalent of a Deputy Secretary.

address the particular requirements described in NIST SP 800-53r1[29], *Recommended Security Controls for Federal Information Systems*. The plans were also to report agencies' current levels of compliance with the current DNSSEC requirements of NIST SP 800-53r1, and document plans of action and milestones that assume the scope of the requirement to operate DNSSEC signed zones. SP 800-53's control SC-20 was required to be expanded to cover all FISMA information systems (including low-impact systems) in its revision 3. The plans were to ensure that all agency .gov domains were DNSSEC-signed by December 2009.

3.10 OMB Memorandum M-11-33: FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

OMB Memorandum M-11-33 includes "Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management." The following frequently asked questions included with the Memorandum are relevant to cryptographic applications:

Must the Department of Defense (DOD) and the Office of the Director of National Intelligence (ODNI) follow OMB policy and NIST guidelines?

Yes, for non-national security systems, DOD and ODNI are to incorporate OMB policy and NIST guidelines into their internal policies.

For national security systems, the Joint Task Force Transformation Initiative (JTFTI) Interagency Working Group, with representatives from the Civil, Defense and Intelligence Communities (IC) started an on-going effort in FY2009 to produce a unified information-security framework for the Federal Government. Under this effort, DOD, ODNI and NIST jointly issued the following publications:

- NIST SP 800-37, Revision 1**,** *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010.
- NIST SP 800-38A, *Recommendation for Block Cipher Modes of Operation,* December 2001.
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* March 2011.
- NIST SP 800-53 Revision 3[30], *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009.

Because these guidelines are jointly issued, DOD and ODNI policies for national security systems should incorporate these guidelines.

Is use of National Institute of Standards and Technology (NIST) publications required?

Yes. For non-national security programs and information systems, agencies must follow NIST standards and guidelines unless otherwise stated by OMB. For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines

[29] The Memorandum referenced an earlier version, Revision 1. The publication has been updated. The current revision is Revision 4.
[30] The Memorandum referenced an earlier version, Revision 3. The publication has been updated. The current revision is Revision 4.

within one year of the publication date unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system.

Are NIST guidelines flexible?

Yes. While agencies are required to follow NIST standards and guidelines in accordance with OMB policy, there is flexibility within NIST's guidelines (specifically in the 800-series) in how agencies apply them. However, NIST Federal Information Processing Standards (FIPS) publications are mandatory. Unless specified by additional implementing policy by OMB, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and compliant with the guidelines.

FISMA, OMB policy, and NIST standards and guidelines require agency security programs to be risk-based. Who is responsible for deciding the acceptable level of risk (e.g., the CIO, program officials and system owners, or the IG)? Are the IGs' independent evaluations also to be risk-based? What if they disagree?

The agency head ultimately is responsible for deciding the acceptable level of risk for their agency. System owners, program officials, and CIOs provide input for this decision. Such decisions must reflect policies from OMB and standards and guidelines from NIST (particularly FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* and FIPS 200, *Minimum Security Requirements for Federal Information and Information Security,* as well as SP 800-39, *Managing Information Security Risk*). An information system' s Authorizing Official takes responsibility for accepting any residual risk, thus they are held accountable for managing the security for that system.

IG evaluations are intended to independently assess that the agency is applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions. For example, when reviewing the assessment in support of an individual security authorization, the IG would generally assess whether: 1) the assessment was performed in the manner prescribed in NIST guidelines and agency policy, 2) controls are being implemented as stated in any planning documentation, and 3) continuous monitoring is adequate given the system impact level of the system and information.

Are there security requirements specific for mobile devices (e.g. smartphones and tablets)?

All existing Federal requirements for data protection and remote access are applicable to mobile devices. For example, the security requirements in OMB Circular A-130, FIPS 140-2, *Security Requirements for Cryptographic Modules,* FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* apply (including appropriate security controls specified in SP 800-53). Agencies should specify

security requirements during the acquisition process and ensure that procurements capture the requirements of the Federal Acquisition Regulation[31] (e.g., 52.225-5, Trade Agreements), OMB policy (e.g., M-06-16 and M-07-16), and NIST standards and guidelines. Additional guidance regarding the use and management of mobile devices will be developed, as appropriate.

3.11 OMB Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements

OMB Memorandum M-16-03 notes that, in early FY 2015, OMB and the National Security Council (NSC) staff created a quarterly cybersecurity assessment organized according to the functions in the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Identify, Protect, Detect, Respond, and Recover)* and associated outcomes to comprehensively assess agency cybersecurity performance. The assessment builds on the existing foundation of FISMA metrics and the Cybersecurity Cross Agency Priority (CAP)[32] goals, and is reviewed by agency senior leadership. Moving forward, the Memorandum states that this assessment will be the cornerstone initiative for how OMB measures Federal agency cybersecurity performance.

[31] Federal Acquisition Regulation, https://www.acquisition.gov/?q=browsefar [accessed 8/8/2016].
[32] *GPRA Modernization Act of 2010, Public Law 111-352,* https://www.performance.gov/cap-goals-list [accessed 8/8/2016].

SECTION 4: ORGANIZATIONAL POLICIES

Every federal organization has (or should have) policies that address the information that they collect or create, including an Information Management Policy and an Information Security Policy. Organizations utilizing cryptography should also have a Key Management Policy.

4.1 Information Management Policy

An organization's Information Management Policy specifies what information is to be collected or created, and how it is to be managed. An organization's management establishes this policy using industry standards of good practices, legal requirements regarding the organization's information, and organizational goals that must be achieved using the information that the organization will be collecting and creating.

An Information Management Policy typically identifies management roles and responsibilities and establishes the authorization required for people performing these information-management duties. It also specifies what information is to be considered sensitive and how it is to be protected. In particular, this policy specifies what categories of information need to be protected against unauthorized disclosure, modification or destruction. These specifications form the foundation for an Information Security Policy and dictate the levels of confidentiality, integrity, availability, and source-authentication protections that must be provided for differing categories of sensitive information (see SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*).

Section 4.1 of SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*, provides requirements for the content of an Information Management Policy for federal agencies.

4.2 Information Security Policy

An organization's Information Security Policy is created to support and enforce portions of the organization's Information Management Policy by specifying in more detail what information is to be protected from anticipated threats and how that protection is to be attained. The rules for collecting, protecting, and distributing sensitive information in both paper and electronic form are specified in this policy. The inputs to the Information Security Policy include, but are not limited to, the Information Management Policy specifications, the potential threats to the security of the organization's information, and the risks involved with the unauthorized disclosure, modification, and destruction or loss of the information.

The outputs of the Information Security Policy include the information sensitivity levels (e.g., low, medium, or high) assigned to various categories of information and the high-level rules for protecting the information (see SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*).

Section 4.2 of SP 800-152 provides requirements for the content of an Information Security Policy for federal agencies.

4.3 Key Management Policies

Each organization that manages cryptographic systems that are intended to protect sensitive information should base the management of the keys used in those systems on an organizational

policy statement. The Key Management Policy includes descriptions of the authorization and protection objectives and constraints that apply to the generation, distribution, accounting, storage, use, recovery and destruction of cryptographic keying material, and the cryptographic services to be provided (e.g., message authentication, digital signature, and encryption).

Further information and requirements for Key Management Policies is provided in Section 3 of SP 800-57 Part 2, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*.

Key-Management Systems manage the cryptographic keys used to protect an organization's sensitive information. Federal organizations may operate their own key-management systems, or may contract for key-management services. Information and requirements on the key management systems that manage cryptographic keys is provided in SP 800-152.

SECTION 5: RISK MANAGEMENT PROCESS

SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*, provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization,[33] security control selection and implementation, security control assessment, information system authorization,[34] and security control monitoring. The guidelines have been developed:

- To ensure that managing information-system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy established by the senior leadership through the risk executive (function);
- To ensure that information security requirements, including the necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes;
- To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity;[35] and
- To achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.

When dealing with cryptographic functions, the tasks involved in applying the Risk Management Framework to information systems focus more on:

- The categorization of information and information systems and the selection of security controls than on the implementation of security controls,
- The assessment of security control effectiveness,
- The authorization of the information system, and
- The ongoing monitoring of security controls and the security state of the information system.

[33] FIPS 199 provides security-categorization guidance for non-national security systems. CNSS Instruction 1253 provides similar guidance for national security systems.

[34] System *authorization* is the official management decision given by a senior organizational official to authorize the operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls.

[35] *Reciprocity* is the mutual agreement among participating organizations to accept each other's security assessments in order to reuse information-system resources and/or to accept each other's assessed security posture in order to share information. Reciprocity is best achieved by promoting the concept of transparency (i.e., making sufficient evidence regarding the security state of an information system available, so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits).

5.1 Categorization of Information and Information Systems

Categorization of information and information systems requires the organization to:

- Categorize the information system and document the results of the security categorization in the security plan as described in FIPS 199; SP 800-30, SP 800-39, SP 800-59, SP 800-60, and CNSS Instruction 1253;
- Describe the information system (including the system boundary) and document the description in the security plan; and
- Register the information system with appropriate organizational program/management offices.

5.2 Selection of Security Controls

The selection of security controls involves the following steps:

- Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document) in accordance with FIPS 199, FIPS 200, SP 800-30, SP 800-53 and CNSS Instruction 1253;
- Select the security controls for the information system and document the controls in the security plan as described in FIPS 199, FIPS 200; SP 800-30, SP 800-53 and CNSS Instruction 1253;
- Develop a strategy for the continuous monitoring of security-control effectiveness and any proposed or actual changes to the information system and its environment of operation as described in SP 800-30, SP 800-39, SP 800-53, SP 800-53A, SP 800-137 and CNSS Instruction 1253; and
- Review and approve the security plan in accordance with SP 800-30, SP 800-53 and CNSS Instruction 1253.

APPENDIX A: REFERENCES

1. Public Law 104-113, *National Technology Transfer and Advancement Act of 1995*, 104th Congress, March 7, 1996. https://www.gpo.gov/fdsys/pkg/PLAW-104publ113/content-detail.html [accessed 8/8/2016].
2. Public Law 107-347, *E-Government Act of 2002*, 107th Congress, December 17, 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf [accessed 8/8/2016].
3. Public Law 111-5, *American Recovery and Reinvestment Act of 2009*, "Health Information Technology for Economic and Clinical Health Act (HITECH Act)," 111th Congress, February 17, 2009. https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf [accessed 8/8/2016].
4. Public Law 111-352, *GPRA Modernization Act of 2010*, 111th Congress, January 4, 2011. https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf [accessed 8/8/2016].
5. Public Law 113-274, *Cybersecurity Enhancement Act of 2014*, 113th Congress, December 18, 2014. https://www.gpo.gov/fdsys/pkg/PLAW-113publ274/content-detail.html [accessed 8/8/2016].
6. Public Law 113-283, *Federal Information Systems Modernization Act of 2014*, 113th Congress, December 18, 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf [accessed 8/8/2016].
7. *National Institute of Standards and Technology*, Title 15 U.S. Code, Sec. 271 *et seq.*, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title15/USCODE-2014-title15-chap7 [accessed 8/8/2016].
8. *Computer standards program*, Title 15 U.S. Code, Sec. 278g-3, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title15/USCODE-2014-title15-chap7-sec278g-3 [accessed 8/8/2016].
9. *Responsibilities for Federal information systems standards*, Title 40 U.S. Code, Sec. 11331, 2014 ed. https://www.gpo.gov/fdsys/granule/USCODE-2014-title40/USCODE-2014-title40-subtitleIII-chap113-subchapIII-sec11331 [accessed 8/8/2016].
10. Executive Office of the President, The White House, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (HSPD-7), December 17, 2003. https://www.dhs.gov/homeland-security-presidential-directive-7 [accessed 8/8/2016].
11. Executive Office of the President, The White House, *Policies for a Common Identification Standard for Federal Employees and Contractors*, Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive-12 [accessed 8/8/2016].
12. Executive Office of the President, The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013. https://federalregister.gov/a/2013-03915 [accessed 8/8/2016].

13. Executive Office of the President, Office of Management and Budget, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, OMB Circular Number A-119, Revised, February 10, 1998. https://www.whitehouse.gov/omb/circulars_a119/ [accessed 8/8/2016].

14. Executive Office of the President, Office of Management and Budget, *Managing Information As a Strategic Resource*, OMB Circular Number A-130, Revised, July 28, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf [accessed 8/8/2016].

15. Executive Office of the President, Office of Management and Budget, *Protection of Sensitive Agency Information*, OMB Memorandum M-06-16, June 23, 2006. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf [accessed 8/8/2016].

16. Executive Office of the President, Office of Management and Budget, *Acquisition of Products and Services for Implementation of HSPD-12*, OMB Memorandum M-06-18, June 30, 2006. https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-18.pdf [accessed 8/8/2016].

17. Executive Office of the President, Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB Memorandum M-07-16, May 27, 2007. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf [accessed 8/8/2016].

18. Executive Office of the President, Office of Management and Budget, *Securing the Federal Government's Domain Name System Infrastruc*ture, OMB Memorandum M-08-23, August 22, 2008. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf [accessed 8/8/2016].

19. Executive Office of the President, Office of Management and Budget, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memorandum M-11-33, September 14, 2011. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf [accessed 8/8/2016].

20. Executive Office of the President, Office of Management and Budget, *Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-16-03, October 30, 2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf [accessed 8/8/2016].

21. Federal Information Processing Standard 140-2 (FIPS 140-2), *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, May 2001 (updated 12/3/2002, Change Notice 2). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 8/8/2016].

22. Federal Information Processing Standard 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of

Standards and Technology, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 8/8/2016].

23. Federal Information Processing Standard 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, National Institute of Standards and Technology, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf [accessed 8/8/2016].
24. Federal Information Processing Standard 201-2 (FIPS 201-2), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, National Institute of Standards and Technology, April 2013. http://dx.doi.org/10.6028/NIST.FIPS.201-2.
25. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2015. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 8/8/2016].
26. National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, NIST Special Publication 800-18 Rev. 1, February 2006. http://dx.doi.org/10.6028/NIST.SP.800-18r1.
27. National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1, September 2012. http://dx.doi.org/10.6028/NIST.SP.800-30r1.
28. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Rev. 1, February 2010 (updated 6/5/2014). http://dx.doi.org/10.6028/NIST.SP.800-37r1.
29. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, NIST Special Publication 800-38A, December 2001. http://dx.doi.org/10.6028/NIST.SP.800-38A.
30. National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. http://dx.doi.org/10.6028/NIST.SP.800-39.
31. National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, NIST Special Publication 800-47, August 2002. http://dx.doi.org/10.6028/NIST.SP.800-47.
32. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 4, April 2013 (updated 1/22/2015). http://dx.doi.org/10.6028/NIST.SP.800-53r4.
33. National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST Special Publication 800-53A, December 2014 (updated 12/18/2014). http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

34. National Institute of Standards and Technology, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*, NIST Special Publication 800-57 Part 2, August 2005. http://dx.doi.org/10.6028/NIST.SP.800-57p2.

35. National Institute of Standards and Technology, *Guideline for Identifying an Information System as a National Security System*, NIST Special Publication 800-59, August 2003. http://dx.doi.org/10.6028/NIST.SP.800-59.

36. National Institute of Standards and Technology, *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST Special Publication 800-60 Rev. 1 (2 vols.), August 2008. http://dx.doi.org/10.6028/NIST.SP.800-60v1r1; http://dx.doi.org/10.6028/NIST.SP.800-60v2r1.

37. National Institute of Standards and Technology, *Electronic Authentication Guideline*, NIST Special Publication 800-63-2, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2.

38. National Institute of Standards and Technology, *Interfaces for Personal Identity Verification*, NIST Special Publication 800-73-4, May 2015 (updated 2/8/2016). http://dx.doi.org/10.6028/NIST.SP.800-73-4.

39. National Institute of Standards and Technology, *Biometric Specifications for Personal Identity Verification*, NIST Special Publication 800-76-2, July 2013. http://dx.doi.org/10.6028/NIST.SP.800-76-2.

40. National Institute of Standards and Technology, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST Special Publication 800-78-4, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-78-4.

41. National Institute of Standards and Technology, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, NIST Special Publication 800-79-2, July 2015. http://dx.doi.org/10.6028/NIST.SP.800-79-2.

42. National Institute of Standards and Technology, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication 800-81-2, September 2013. http://dx.doi.org/10.6028/NIST.SP.800-81-2.

43. National Institute of Standards and Technology, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73-4 Compliance)*, NIST Special Publication 800-85A-4, April 2016. http://dx.doi.org/10.6028/NIST.SP.800-85A-4.

44. National Institute of Standards and Technology, *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Rev. 1, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-88r1.

45. National Institute of Standards and Technology, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, NIST Special Publication 800-116, November 2008. http://dx.doi.org/10.6028/NIST.SP.800-116.

46. National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST Special Publication 800-122, April 2010. http://dx.doi.org/10.6028/NIST.SP.800-122.

47. National Institute of Standards and Technology, *A Framework for Designing Cryptographic Key Management Systems*, NIST Special Publication 800-130, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-130.

48. National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication 800-137, September 2011. http://dx.doi.org/10.6028/NIST.SP.800-137.

49. National Institute of Standards and Technology, *A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)*, NIST Special Publication 800-152, October 2015. http://dx.doi.org/10.6028/NIST.SP.800-152.

50. National Institute of Standards and Technology, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST Special Publication 800-157, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-157.

51. National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST Special Publication 800-161, April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161.

52. National Institute of Standards and Technology, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication 800-162, January 2014. http://dx.doi.org/10.6028/NIST.SP.800-162.

53. National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication 800-171, June 2015 (updated 1/14/2016). http://dx.doi.org/10.6028/NIST.SP.800-171.

54. National Institute of Standards and Technology, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, NIST Special Publication 800-175B, August 2016. http://dx.doi.org/10.6028/NIST.SP.800-175B.

55. Committee on National Security Systems (CNSS), *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253, March 27, 2014. Available at: https://www.cnss.gov/CNSS/issuances/Instructions.cfm [accessed 8/8/2016].

56. National Institute of Standards and Technology, and the Communications Security Establishment Canada, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, CMVP, March 28, 2003, Last Update June 17, 2016. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf [accessed 8/8/2016].

57. National Institute of Standards and Technology, *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*, June 2014. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/nist_oa_guidance.pdf [accessed 8/8/2016].