The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-175A**

Title: **Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies**

Publication Date: **8/22/2016**

- Final Publication: *http://dx.doi.org/10.6028/NIST.SP.800-175A* (which links to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf).

- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

April 5, 2016

NIST requests comments on Draft Special Publication (SP) 800-175A, Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies

NIST requests comments on Draft Special Publication (SP) 800-175A, Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies. The SP 800-175 publications are intended to be a replacement for SP 800-21, Guideline for Implementing Cryptography in the Federal Government. SP 800-175A provides guidance on the determination of requirements for using cryptography. It includes a summary of the 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). Please provide comments on SP 800-175A by Monday, May 9, 2016. Comments may be sent to SP800-175@nist.gov, with "Comments on SP 800-175A" as the subject.

Draft NIST Special Publication 800-175A

Guideline for Using Cryptographic Standards in the Federal Government:

Directives, Mandates and Policies

Elaine Barker
William C. Barker

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

Draft 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
Information Technology Laboratory

April 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 (FISMA) of 2014, 44 U.S.C. § 3541 *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, 32 pages (April 2016)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *April 5, 2016* through *May 9, 2016*

All comments are subject to release under the Freedom of Information Act (FOIA).

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.

137 **Table of Contents**

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	A process that provides assurance of the source and integrity of information that is communicated or stored.
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 for an other than authorized purpose 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 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 and 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.
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.
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 possession of a physical or software token in combination with some memorized secret knowledge.

1.3 Acronyms

C&A – Certify and Accredit

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

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

ITL – Information Technology Laboratory

JTFTI – Joint Task Force Transformation Initiative

NIST – National Institute of Standards and Technology

NPIVP– NIST Personal Identity Verification Program

NSA – National Security Council

ODNI – Office of the Director of National Intelligence

OMB – Office of Management and Budget

PHI – Protected Health Information

PIV – Personal Identity Verification

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 1) 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 and has been incorporated into Sections 20 and 21 of the NIST Organic 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 potential 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 part 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. 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[1].

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] 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 format 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 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 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 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 law, 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.

3.3 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 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 CircularA-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: Management of Federal Information Resources

OMB Circular A-130 establishes policy for the management of federal information resources. A-130 includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices. Section 8 of the Circular requires that agencies' Information Technology Capital Plans explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance. Specifically, the Circular directs the certification and accreditation of federal information systems and mandates Agency-wide Information Security Program development and implementation.

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 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 NPVIP Test Facilities.

FIPS 140-2: *Security Requirements for Cryptographic Modules,* 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[2] 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:

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, or 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 (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, 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 SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*,[3] 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).

[2] 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.

[3] Since reissued as *Guide for Applying the Risk Management Framework for Federal Information Systems: A Security Life Cycle Approach.*

The Memorandum's requirements include 1) encryption using only NIST-certified cryptographic modules[4] 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[5] 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 requires 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 address the particular requirements described in NIST SP 800-53r1, *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

[4] See NIST's website at http://csrc.nist.gov/cryptval/ for a discussion of the validated encryption modules.

[5] Non-cabinet agencies should consult the equivalent of a Deputy Secretary.

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, *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 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 publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* and FIPS publication 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 (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 Requirement

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)*[6] 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)[7] 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.

[6] http://www.nist.gov/cyberframework/

[7] *GPRA Modernization Act of 2010, Public Law 111-352*, https://www.performance.gov/cap-goals-list

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, and high) assigned to various categories of information and 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

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

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

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

855

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,[8] security control selection and implementation, security control assessment, information system authorization,[9] 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 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;[10] 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.

5.1 Categorization of Information and Information Systems

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

[9] 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.

[10] *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).

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]
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]
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]
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]
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]
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]
7. Executive Office of the President, The White House, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive 7 (HSPD-7), December 17, 2003. [http://itlaw.wikia.com/wiki/Homeland_Security_Presidential_Directive_7]
8. 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]
9. Executive Office of the President, The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, February 12, 2013. [https://fas.org/irp/offdocs/eo/eo-13636.htm]
10. 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*, Memorandum for the Heads of Departments and Agencies, Circular Number A-119, Revised, February 10, 1998. [https://www.whitehouse.gov/omb/circulars_a119/]
11. Executive Office of the President, Office of Management and Budget, *Management of Federal Information Resources*, Memorandum for the Heads of Departments and Agencies, Circular Number A-130, Revised, November 8, 2000. [https://www.whitehouse.gov/omb/circulars_a130_a130trans4/]

12. Executive Office of the President, Office of Management and Budget, *Protection of Sensitive Agency Information*, Memorandum for the Heads of Departments and Agencies, M-06-16, June 23, 2006. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf]

13. Executive Office of the President, Office of Management and Budget, *Acquisition of Products and Services for Implementation of HSPD-12*, Memorandum For Chief Information Officers Chief Acquisition Officers Chief Financial Officers, M-06-18, June 30, 2006. [https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-18.pdf]

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

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

16. 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*, Memorandum for the Heads of Departments and Agencies, M-11-33, September 14, 2011. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf]

17. Executive Office of the President, Office of Management and Budget, *Guidance on Federal Information Security and Privacy Management Requirement*, Memorandum for the Heads of Departments and Agencies, M-16-03, October 30, 2015. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf]

18. Federal Information Processing Standard 140-2 (FIPS 140-2), *Security Requirements for Cryptographic Modules*, Department of Commerce, May 2001. [http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf]

19. Federal Information Processing Standard 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, Department of Commerce, February 2004. [http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf]

20. Federal Information Processing Standard 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, Department of Commerce, March 2006. [http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf]

21. Federal Information Processing Standard 201-2 (FIPS 201-2), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Department of Commerce, April 2013. [http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf]

22. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2015. [http://www.nist.gov/cyberframework/]

23. National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1, September 2012. [http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf]

24. 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. [doi:10.6028/NIST.SP.800-37r1]

25. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, NIST Special Publication 800-38A, December 2001. [http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf]

26. National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. [http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf]

27. 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. [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf]

28. 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. [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf]

29. 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://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf]

30. 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, August 2008. [http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf]

31. National Institute of Standards and Technology, *Interfaces for Personal Identity Verification*, NIST Special Publication 800-73-4, May 2015. [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf]

32. National Institute of Standards and Technology, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication 800-81-2, September 2013. [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf]

33. National Institute of Standards and Technology, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73-3 Compliance)*, NIST Special Publication 800-85A, July 2010. [http://csrc.nist.gov/publications/nistpubs/800-85A-2/sp800-85A-2-final.pdf]

34. National Institute of Standards and Technology, *A Framework for Designing Cryptographic Key Management Systems*, NIST Special Publication 800-130, August 2013. [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf]

35. National Institute of Standards and Technology, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, NIST Special Publication 800-137, September 2011. [http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf]

36. 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf]

37. National Institute of Standards and Technology, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, DRAFT NIST Special Publication 800-175B, March 2016. [http://csrc.nist.gov/publications/drafts/800-175/sp800-175b_draft.pdf]

38. Committee on National Security Systems (CNSS), Security. *Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253, October 2009. [https://www.cnss.gov/CNSS/openDoc.cfm?nHul5v6UB1ZgyvIilIN/6g==]