CHIEF INFORMATION SECURITY OFFICER

HANDBOOK

CONTENTS

EXECUTIVE SUMMARY

DOCUMENT OBJECTIVES

- Educate and inform new and existing Chief Information Security Officers (CISOs) about their role in successfully implementing Federal cybersecurity.
- Provide resources to help CISOs responsibly apply risk management principles to help Federal agencies meet mission objectives.
- Make CISOs aware of laws, policies, tools, and initiatives that can assist them as they develop or improve cybersecurity programs for their organizations.

This handbook aims to give CISOs important information they will need to implement Federal cybersecurity at their agencies. It is designed to be useful both to an executive with no Federal Government experience and to a seasoned Federal employee familiar with the nuances of the public sector. At its core, the handbook is a collection of resources that illuminate the many facets of the cybersecurity challenge and the related issues and opportunities of Federal management.

Section 1 outlines the CISO's role within the agency and in the Federal Government as a whole. The section starts with an overview of the statutory language that defines the CISO's mandate and the responsibilities agencies have in regard to information and information security. Next comes an overview of key organizations and their roles in Federal cybersecurity. The section concludes with a summary of the many kinds of reporting the CISO must conduct to keep the agency accountable to government-wide authorities.

In Section 2, the challenge of cybersecurity is broken down into two parts: managing risk across the enterprise and government-wide policies and initiatives. Each part begins with summaries of key reference documents for that aspect of the challenge.

The risk management portion of Section 2 uses as its guide The Framework for Improving Critical Infrastructure Cybersecurity, agencies' implementation of which was mandated by Executive Order 13800. To provide a systematic overview of the risk management process, example agency policies are mapped to specific objectives in the Cybersecurity Framework Core as well as to key National Institute of Standards and Technology (NIST) publications.

Section 2 concludes with examples of government-wide approaches to cybersecurity. These examples show how an initiative or threat can be translated into policy that must then be incorporated into agency-level operations and policy.

Section 3 contains information to help CISOs manage their organization's resources. The section begins with an overview of Federal workforce and hiring authorities and the mechanisms by which a CISO can develop an effective cybersecurity team. An overview of contracting follows with summaries of Federal acquisition regulations and

EXECUTIVE SUMMARY (CONT)

contracting vehicles. Section 3 ends with a high-level overview of the government-wide services designed to help CISOs better perform their duties and improve the cybersecurity posture of their agency and, by extension, the Federal Government as a whole.

The appendices contain links and reference documents that direct CISOs to more detailed information on the tools, policies, and best practices discussed in this handbook. The "FISMA Responsibility Breakdowns" and the "Government-wide Policies and Publications" portion were developed specifically for this handbook.

As a whole, this handbook is meant to provide CISOs with a foundational understanding of their role. The information is presented in plain language with the expectation that it will be reinforced with detailed analysis of both government-wide and agency-specific resources. The tools, initiatives, policies, and links to more detailed information make the handbook an effective reference document regardless of the reader's familiarity with Federal cybersecurity.

ACKNOWLEDGEMENTS

This handbook would not have been possible without the contributions and efforts of the CISO Handbook Federal Working Group, which included representatives from the Office of Personnel Management, the Department of Health and Human Services Centers for Medicare and Medicaid Services, the Office of Management and Budget's Office of the Federal Chief Information Officer, the Chief Information Officer/Chief Information Security Officer Council and the General Services Administration's Office of Government-wide Policy. Thanks to Incapsulate, LLC and REI Systems, Inc. for developing the content of the handbook, and to Eagle Hill Consulting for their work in formatting and graphics.

CISO ROLES & RESPONSIBILITIES

SECTION 1

1.1 The CISO Role at a Glance
1.2 Overview of Key Organizations
1.3 Reporting Requirements

1.1 THE CISO ROLE AT A GLANCE

The CISO's Legislative Mandate: FISMA 2014

The Federal Information Security Modernization Act of 2014

WHAT THE LAW SAYS

The Federal Information Security Modernization Act of 2014 (FISMA)[1] states:

Under **§ 3554. Federal agency responsibilities**

IN GENERAL.—The head of each agency shall— (1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

[…]

(C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes.

IN GENERAL.—The head of each agency shall—(3) delegate to the agency Chief Information Officer…the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section

The head of each agency has a legislative mandate to maintain and improve the security of their agency's information and information systems. In most cases, the agency's internal policies delegate management of the agency's information to the Chief Information Officer (CIO). Under FISMA, the CIO may then delegate tasks related to information security to the senior agency information security officer (often referred to as CISO).

[1]For the purposes of this document, "FISMA" will refer the 2014 law, not the Federal Information Security Management Act of 2002.

1.1 THE CISO ROLE AT A GLANCE

LEGISLATIVE MANDATE

The head of each agency has a legislative mandate to maintain and improve the security of their agency's information and information systems. In most cases, the agency's internal policies delegate management of the agency's information to the Chief Information Officer (CIO). Under FISMA, the CIO may then delegate tasks related to information security to the senior agency information security officer (often referred to as CISO).

THINGS TO KNOW

- Agencies may organize their information security reporting structure in different ways, but ultimately all information security functions are the responsibility of the agency head. (*See* Agency-wide Information Security Tasks)
- Reporting requirements, breach and major incident responsibilities, and other functions may be directly called out in legislation or indirectly established through organizational authorities.
- FISMA also defines the government-wide information security roles played by key organizations (e.g. Office of Management and Budget, Department of Homeland Security). For a complete breakdown of these roles, see "FISMA Responsibility Breakdowns" in Section A.3 of the appendices.

1.1 THE CISO ROLE AT A GLANCE

AGENCY-WIDE INFORMATION SECURITY TASKS

While FISMA requires agencies to delegate information security tasks to their respective CISOs, those tasks are not organized in the same manner at each agency. FISMA does not instruct agencies on how to develop or maintain their information security programs; it simply lists agencies' information security responsibilities. Agencies are encouraged to approach compliance with government-wide requirements in a manner that fits their respective missions and resource capabilities.

Because no two agency missions are exactly the same, no two CISO roles are exactly the same. Some CISOs are responsible for all information security tasks at their agency, while others work with separate operations centers or take on tasks outside of information security to help with organizational priorities.[2] Although FISMA allows for these nuances, CIOs and CISOs are ultimately statutorily responsible for information security, so they must be aware of the range of information security responsibilities assigned to agencies.

The following are some of the key information security responsibilities assigned to agencies as a whole. Depending on the agency, these tasks may or may not fall entirely or exclusively to the CISO.

- Agencies must comply with:
  - ◊ Executive Orders or Presidential Memoranda issued by the President and with policies or guidance issued by the Office of Management and Budget (OMB). Those issued by the President will often be accompanied or followed by OMB guidance and implementation timelines. (*See* *Section 1.2.* Office of Management and Budget)
  - ◊ Minimum security requirements and standards promulgated by the NIST. (*See* *Section 1.2.* National Institute of Standards and Technology)
  - ◊ Binding operational directives (BODs) developed by the Department of Homeland Security (DHS). These directives are developed in response to a known or reasonably suspected information security threat, vulnerability or risk. (*See* *Section 1.2.* Department of Homeland Security)
- Agencies must develop and maintain an agency-wide information security program that can perform the following functions:
  - ◊ The agency must be able to assess risk and determine the appropriate level of protections for assets. NIST publications are designed to help agencies assess risk. Once the proper controls are in place, they must be periodically tested and evaluated to ensure compliance.
  - ◊ The agency must develop and maintain information security policies, procedures, and control techniques to address all applicable government-wide requirements. Examples of agency policy and procedure development can be found in Section 2.
  - ◊ The agency must comply with Federal reporting requirements including progress on remedial actions (typically called Plan of Action and Milestones (POA&M)).
  - ◊ The agency must develop plans and procedures to ensure continuity of operations for information

[2] In a December 2017 survey of CISOs, several respondents listed responsibilities outside of information security. Examples of those responsibilities include Deputy CIO duties, privacy and privacy incident response, Controlled Unclassified Information (CUI) duties, and healthcare sector outreach.

systems that support the operations and assets of the agency.

- ◊ The agency must ensure information security staff members are trained and that all agency personnel are held accountable for complying with the agency-wide information security program. Workforce management is addressed in Section 3.

- Additional agency responsibilities include:
  - ◊ Reporting breaches and major incidents to the US-Computer Emergency Readiness Team operated by DHS within mandatory timelines. (*See Section 1.3.* Reporting Requirements)
  - ◊ Ensuring CISOs have the appropriate professional qualifications to lead information security across the agency as their primary responsibility, implement cybersecurity solutions where necessary, and ensure their office directs its mission and resources toward enhancing agency cybersecurity.

1.2 OVERVIEW OF KEY ORGANIZATIONS

The Office of Management and Budget (OMB)

WHAT THE LAW SAYS

FISMA states:

Under **§ 3553. Authority and functions of the Director [OMB] and the Secretary [DHS]**

DIRECTOR.—The Director [OMB] shall oversee agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security […]

Under **§ 3553. Authority and functions of the Director [OMB] and the Secretary [DHS]**

REPORT.—Not later than March 1 of each year, the Director [OMB], in consultation with the Secretary [DHS], shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year […]

Under **§ 3555. Annual independent evaluation**

AGENCY REPORTING.—Each year, not later than such date established by the Director [OMB], the head of each agency shall submit to the Director [OMB] the results of [their agency's] evaluation required under this section.

OMB OVERVIEW

OMB is responsible for overseeing Federal agencies' information security practices. As part of this core function, OMB develops and ensures implementation of policies and guidelines that drive enhanced cybersecurity performance and budgeting across the Executive Branch. The Federal Chief Information Security Officer (Federal CISO) leads the OMB Cyber and National Security Unit (OMB Cyber). OMB Cyber is the dedicated team within the Office of the Federal Chief Information Officer (OFCIO) that works with Federal agency leadership to address information security priorities. OMB Cyber partners with DHS to develop cybersecurity policies, conduct data-driven oversight of agency cybersecurity programs, and coordinate the Federal response to cyber incidents.[3]

[3] FISMA Annual Report to Congress FY2016
https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

1.2 OVERVIEW OF KEY ORGANIZATIONS

THINGS TO KNOW

- OMB OFCIO:
  - ◊ Guides cybersecurity policy, planning, and implementation in the Federal Government.
  - ◊ Reports to the Federal Chief Information Officer (Federal CIO).
  - ◊ Leads cyber response and communication efforts as well as communication with Congress and the public.
  - ◊ Partners with the Office of Information and Regulatory Affairs (OIRA) to address related privacy concerns such as System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs), including Third Party Web Application PIAs. Circular A-130 also contains specific government-wide privacy requirements.[4]
- OMB partnership with DHS:
  - ◊ OMB works closely with DHS to collect reports on cybersecurity incidents, readiness, and compliance with cybersecurity policies.
  - ◊ OMB and DHS partner to define agency performance and drive change both government-wide and within agencies through annual statutory FISMA metrics and other OMB- and DHS-developed processes and programs.
- Additional OMB roles and responsibilities:
  - ◊ FISMA authorizes OMB to define the term "major incident" and further directs agencies to notify Congress of a major incident, a process in which the Federal CISO is heavily involved. The most recent definition is provided in OMB M-18-02, while guidance for agency incident handling can be found in The US-CERT Federal Incident Notification Guidelines.

[4]Privacy Act of 1974, 5 U.S.C. § 552a
https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf
Circular A-130 – Managing Information as a Strategic Resource
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
M-17-06 – Policies for Federal Agency Public Websites and Digital Services
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf
M-10-22 – Guidance for Online Use of Web Measurement and Customization Technologies
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-22.pdf
M-10-23 – Guidance for Agency Use of Third-Party Websites and Applications
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

1.2 OVERVIEW OF KEY ORGANIZATIONS

THINGS TO KNOW (CONT)

- OIRA is responsible for providing assistance to Federal agencies on privacy matters, developing Federal privacy policy, and overseeing implementation of privacy policy by Federal agencies in coordination with OMB Cyber.
- OMB drives outcomes related to Presidential directives. For example, in response to Executive Order 13800, the recent Report to the President on Federal IT Modernization made recommendations for modernizing Federal networks (such as prioritizing High Value Assets and Trusted Internet Connections) and expanding the use of shared and cloud-based services.[5]
- Budget planning and execution is another of OMB's critical missions. OMB issues detailed annual budget guidance to agencies in the form of Circular A-11 and accompanying memos. Because budgets must be planned two years in advance, CISOs must be aware of new guidance and also be prepared to justify budgetary requests.
- Cross Agency Priority (CAP) Goals, established by the President's Management Agenda, are a management tool used to accelerate progress on objectives that require both senior leadership focus and the coordination of multiple agencies. The CAP Goal mechanism helps coordinate cross-agency collaboration to achieve mission outcomes. The current cycle of four-year outcome-oriented objectives will run from FY2018 through FY2021.

[5]Executive Order 13800 – https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical infrastructure/
Report to the President on Federal IT Modernization – https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

1.2 OVERVIEW OF KEY ORGANIZATIONS

Department of Homeland Security (DHS)

WHAT THE LAW SAYS

FISMA states:

Under **§ 3553. Authority and functions of the Director [OMB] and the Secretary [DHS]**

Secretary [DHS].—The Secretary [DHS], in consultation with the Director [OMB], shall administer the implementation of agency information security policies and practices for information systems

[…] including assisting the Director [OMB] in carrying out the authorities and functions under [the subsection establishing the Director [OMB]'s authority and functions

[…] including developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director [OMB] […]

Under **§ 3556. Federal information security incident center**

IN GENERAL.—The Secretary [DHS] shall ensure the operation of a central Federal information security incident center to […] provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents […]

The Federal Cybersecurity Enhancement Act states:

Under **§ 1524. Assessment; reports,**

(A) Secretary of Homeland Security report—Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities[…]

DHS OVERVIEW

FISMA designates DHS as the operational lead for Federal cybersecurity and provides DHS authority to coordinate government-wide cybersecurity efforts. DHS issues binding operational directives (BODs) to agencies on actions to improve their cybersecurity as part of this coordination of efforts. DHS also provides operational and technical assistance to agencies through the operation of the Federal information security incident center and other tools (*See Section 3.3*).[6] The FY19 budget includes $1.0 billion to support DHS's efforts to safeguard the Federal Government's civilian information technology systems against cybersecurity threats. These funds also support DHS efforts to share cybersecurity information with state, local, and tribal governments, as well as with international partners and the private sector.[7]

[6] FISMA Annual Report to Congress FY2016 https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

[7] Budget Of The U. S. Government for Fiscal Year 2019 https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf

1.2 OVERVIEW OF KEY ORGANIZATIONS

THINGS TO KNOW

- DHS develops and oversees the implementation of BODs. These are developed in consultation with OMB to implement the policies, principles, standards, and guidelines developed by OMB in accordance with FISMA and other authorities. BODs target government-wide action, whether in response to a specific threat or a policy directive from the President. DHS also partners with NIST to ensure BODs align with government-wide standards.[8]
- DHS provides incident response assistance to all Federal Agencies in accordance with Presidential Policy Directive 41 (PPD-41)and FISMA. DHS operates the Federal Information Security incident center known as US-CERT (*See* Focus on: National Cybersecurity and Communications Integration Center). US-CERT's critical mission activities include:
    - ◊ Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
    - ◊ Developing timely and actionable information for distribution to Federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
    - ◊ Responding to incidents and analyzing data about emerging cybersecurity threats.
- DHS provides common security capabilities and tools for agencies:
    - ◊ The National Cybersecurity Protection System (commonly known as "EINSTEIN") detects and blocks cyber attacks from compromising Federal agencies. It also provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the Government and to help the private sector protect itself.
- Presidential Policy Directive 21 (PPD-21) spells out the policy for how the Federal Government builds trusted partnerships with the private sector. It identifies 16 critical infrastructure sectors and designates associated Federal Sector-Specific Agencies (SSAs) to lead each public-private partnership. DHS is the designated SSA for many sectors,

[8]Federal Information Security Modernization Act of 2014, 35 U.S.C. § 3553
[9]Presidential Policy Directive-21 – Critical Infrastructure Security and Resilience https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

1.2 OVERVIEW OF KEY ORGANIZATIONS

THINGS TO KNOW (CONT)

◊ The Continuous Diagnostics and Mitigation (CDM) program provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

◊ In addition to the protection provided by US-CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)'s assessment products improve situational awareness and provide insight, data, and identification of control systems threats and vulnerabilities. ICS-CERT's core assessment products and services include self-assessments using ICS-CERT's Cybersecurity Evaluation Tool (CSET). CSET provides an excellent means to perform a self-assessment of the security posture of an agency's control system environment.

◊ Conducts Federal Cybersecurity Coordination, Assessment, and Response (C-CAR) calls to ensure that agency CIOs and CISOs are empowered with the necessary information to drive critical detection or mitigation activities across their agencies and provide DHS with the information necessary to understand government-wide risk.

- Additional DHS responsibilities:

◊ Operates the Trusted Internet Connections (TIC) Initiative to optimize and standardize the security of individual external network connections currently in use by Federal agencies, including connections to the Internet.

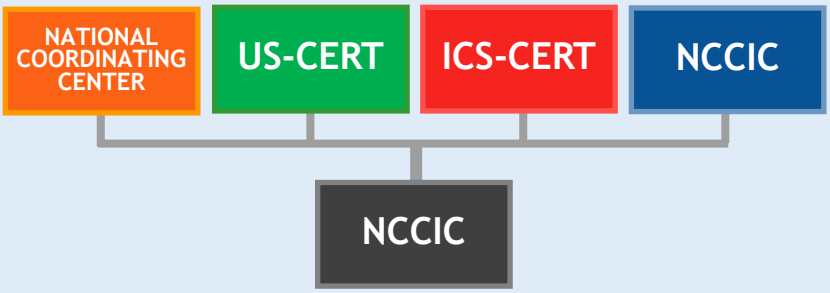
◊ Facilitates Automated Indicator Sharing (AIS) across the Federal Government and the private sector, in accordance with the Cybersecurity Information Sharing Act (CISA) of 2015.

including Information Technology. Cross-sector coordination is handled by the NSC.[9]

1.2 OVERVIEW OF KEY ORGANIZATIONS

Focus On: National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC within DHS serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC recently reorganized its legacy organizations, US-CERT and ICS-CERT, into a streamlined entity. More information on their organizational realignment and mission can be found in NCCIC Year in Review: FY 2017.



NCCIC collaborates closely with its constituent departments and agencies to help them take action to mitigate cyber risk. Federal departments and agencies are also major contributors to NCCIC's cyber and communications security capabilities.

NCCIC coordinates with various federal organizations—particularly Sector-Specific Agencies, the Office of Management and Budget, other DHS organizations, and the intelligence and law enforcement communities—on a broad range of operational activities. For example, NCCIC maintains close operational relationships with other federal cybersecurity centers and federal security operations centers (SOCs). These include the following:

- Cyber Threat Intelligence Integration Center (Office of the Director of National Intelligence)
- U.S. Cyber Command Joint Operations Center (Department of Defense);
- Department of Defense Cyber Crime Center (DC3);
- National Cyber Investigative Joint Task Force (Federal Bureau of Investigation);
- Intelligence Community-Security Coordination Center;
- National Security Agency (NSA) Central Security Service Threat Operations Center; and
- various federal SOCs (e.g., Transportation Security Administration SOC).

During major incidents, or in response to sustained cyber campaigns and challenges, NCCIC spearheads DHS coordination and collaboration with departments and agencies (as outlined in PPD-41). They provide situational awareness and advice to DHS leadership and senior government officials, Congress, and the National Security Council.

1.2 OVERVIEW OF KEY ORGANIZATIONS

National Institute of Standards and Technology (NIST)

WHAT THE LAW SAYS

FISMA states:

Under **§ 3553. Authority and functions of the Director [OMB] and the Secretary [DHS]**

CONSIDERATION.—IN GENERAL.—In carrying out the responsibilities [under this subsection], the Secretary [DHS] shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce [...]

CONSIDERATION.—DIRECTIVES.—The Secretary [DHS] shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology;

The National Institute of Standards and Technology Act states:

Under **§ 278g–3. Computer standards program,**

IN GENERAL.—The Institute shall—

(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 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, but such standards and guidelines shall not apply to national security systems.

NIST OVERVIEW

A bureau of the Department of Commerce, NIST provides Federal standards and technical resources on information security that CISOs use to ensure agencies effectively manage risk and the Offices of Inspector General (OIG) uses to evaluate maturity. OMB and DHS leverage NIST guidance as they develop mandates and initiatives. NIST creates mandatory Federal Information Processing Standards (FIPS) and provides management, operational, and technical security guidelines on a broad range of topics, including incident handling and intrusion detection, the establishment of security control baselines, and strong authentication.

1.2 OVERVIEW OF KEY ORGANIZATIONS

THINGS TO KNOW

- NIST publications are collected online in the Computer Security Resource Center (CSRC). NIST develops standards and guidance through a deliberative process with both Federal and civilian input.
    - ◊ Federal Information Processing Standards (FIPS) establish mandatory requirements for information processing.[10]
    - ◊ NIST Special Publications (SPs) provide guidance for developing agency-wide information security programs, including guidelines, technical specifications, recommendations, and reference materials. NIST SPs comprise multiple sub-series:
        - ♦ The NIST SP 800-series focuses on computer security, and
        - ♦ The NIST SP 1800-series provides cybersecurity practice guides.
    - ◊ NIST Internal or Interagency Reports (NISTIRs) are reports of research findings, including background information for FIPS and SPs.
    - ◊ NIST Information Technology Laboratory Bulletins (ITL Bulletins) are monthly overviews of NIST's security and privacy publications, programs, and projects.
- The Framework for Improving Critical Infrastructure Cybersecurity (referred to as the NIST Cybersecurity Framework) provides a common taxonomy and mechanism for organizations to:
    - ◊ Describe their current and target cybersecurity postures,
    - ◊ Identify and prioritize opportunities for improvement,
    - ◊ Assess progress toward their target, and
    - ◊ Communicate among internal and external stakeholders about cybersecurity risk.
- Each agency's Office of Inspector General (OIG) considers FIPS and SPs when evaluating the effectiveness of agency information security programs. NIST encourages tailoring of guidance to agency needs. OIG expects those tailoring decisions and associated risk decisions to be reflected in the organization's policies, procedures, and guidance.
- The NIST Risk Management Framework (RMF) provides a foundational process that integrates security and risk management activities into the system development life cycle and brings many of the NIST documents together into an overall approach to managing risk.
- NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, Government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues.

[10] 40 U.S.C. §11331. Responsibilities for Federal information systems standards

1.2 OVERVIEW OF KEY ORGANIZATIONS

General Services Administration

GSA OVERVIEW

GSA provides management and administrative support to the entire Federal Government and establishes acquisition vehicles for agencies' use. GSA's information technology acquisition services and offerings are updated along with government-wide policy and are offered through collaboration with DHS, OMB, and other organizations both inside and outside the Federal Government.

THINGS TO KNOW (CONT)

- GSA's Highly Adaptive Cybersecurity Services (HACS) streamlines the acquisitions process for cybersecurity risk assessments that follow the DHS National Cybersecurity Assessments and Technical Services (NCATS) standards (*See* Section 3.2).
- The Federal Identity, Credential, and Access Management (FICAM) program provides collaboration opportunities and guidance on IT policy, standards, implementation and architecture to help Federal agencies implement identity, credential, and access management (ICAM) policy.
- GSA maintains common platforms for government-wide use such as login.gov, cloud.gov, IDManagement.gov, and others.
- GSA's Office of Information Technology Category (ITC) provides integrated, solutions-based telecommunications and IT infrastructure services that blend telecommunications technologies. The Enterprise Infrastructure Solutions (EIS) program is a comprehensive solution-base vehicle to address all aspects of federal agency IT telecommunications, and infrastructure requirements.
- The Federal Risk and Authorization Management Program (FedRAMP) program provides information on Federal authorization requirements for cloud computing. (*See* Section 3.2) .

1.2 OVERVIEW OF KEY ORGANIZATIONS

GSA collaborates with OMB to sponsor Executive Councils for inter-agency communication and also assist. OMB in the development of government-wide policies and guidance. The councils vary significantly in their scope and subject matter, but they all serve three core functions:

- To create communities of practice that can share approaches, solutions and lessons learned across government so that success in one agency can be shared across the enterprise
- To provide a venue for feedback on policy development based on the perspective and experience of on the ground practitioners
- To solve systemic management challenges that require collaboration across organizational and functional silos

1.2 OVERVIEW OF KEY ORGANIZATIONS

Independent Bodies

Office of Inspector General (OIG)

WHAT THE LAW SAYS

Under **§ 3555. Annual independent evaluation,** FISMA states:

IN GENERAL.— Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

Under **§ 3555. Annual independent evaluation,** FISMA also states:

INDEPENDENT AUDITOR.—Subject to subsection (c)— for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.

OIG OVERVIEW

FISMA requires each agency's Inspector General (IG) or an independent external auditor to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. The metrics for these evaluations are updated annually through a collaboration between OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal CIO Council. OIGs are valuable partners to CISOs because they help provide an independent view of agency-wide cybersecurity programs. They can help identify weaknesses and areas for improvement.

Government Accountability Office (GAO)

WHAT THE LAW SAYS

FISMA states:

Under **§ 3555. Annual independent evaluation**

COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on— the adequacy and effectiveness of agency information security policies and practices

GAO OVERVIEW

The GAO, headed by the Comptroller General of the United States, is an independent, nonpartisan agency that works for Congress. As part of their mission to investigate how the Federal Government spends taxpayer dollars, they conduct evaluations of agencies' information security policies and practices.[12] Their primary method of evaluation is the Federal Information System Controls Audit Manual (FISCAM), which is consistent with the NIST Cybersecurity Framework.

[12] About GAO https://www.gao.gov/about/index.html

1.2 OVERVIEW OF KEY ORGANIZATIONS

National Security

National Security Council (NSC)

WHAT THE LAW SAYS

TITLE 50—SUBCHAPTER I—COORDINATION FOR NATIONAL SECURITY states:

Under **§ 3021. National Security Council**

> In addition to performing such other functions as the President may direct, for the purpose of more effectively coordinating the policies and functions of the departments and agencies of the Government relating to the national security, it shall, subject to the direction of the President, be the duty of the Council [...] to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith.

NSC OVERVIEW

The NSC Cybersecurity Directorate advises the President of United States on cybersecurity issues from a national security and foreign policy perspective and is part of the executive office of the President.[13] In accordance with PPD-41, the NSC Cyber Response Group (CRG) coordinates with OMB and collaborates with Federal agencies to implement the Administration's Federal cybersecurity priorities. The CRG supports the NSC Deputies and Principals Committees and is accountable through the Assistant to the President for Homeland Security and Counterterrorism (APHSCT).[14] The NSC champions government-wide cybersecurity initiatives and may also facilitate sector engagement when an initiative, incident, or other situation requires such coordination.

Federal Bureau of Investigation (FBI)

FBI OVERVIEW

The FBI is the component of the Department of Justice responsible for leading Federal investigations of cybersecurity intrusions and attacks carried out against public and private targets by criminals, overseas adversaries, and terrorists. The FBI's capabilities and resources for handling cybersecurity-related issues include a Cyber Division, globally deployable Cyber Action Teams, and partnerships with Federal, state, and local law enforcement, and cybersecurity organizations.[15]

---

[13] FISMA Annual Report to Congress FY2016 https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

[14] Presidential Policy Directive 41 – United States Cyber Incident Coordination https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[15] FISMA Annual Report to Congress FY2016 https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

1.3 REPORTING REQUIREMENTS

Annual Reporting Schedule

	FY Q1	FY Q2	FY Q3	FY Q4
Estimated Deadline	January	April	July	October
Reporting	Q1 CIO FISMA Reporting Annual HVA Reporting	Q2 CIO FISMA Reporting	Q3 CIO FISMA Reporting	Annual CIO FISMA Reporting Annual IG FISMA Reporting Annual Senior Agency Official for Privacy (SAOP) FISMA Reporting
Responsible Parties	CFO Act Agencies (required) Small agencies (optional)	All Civilian Agencies	CFO Act Agencies (required) Small agencies (optional)	All Civilian Agencies

ANNUAL REPORTING OVERVIEW

Under FISMA, agencies are responsible for conducting annual and periodic evaluations of their information security systems and submitting reports to DHS. Reporting metrics for the coming fiscal year are released in Q4. Current metrics for CIO, IG, and SAOP reporting can be found on the DHS website, along with submission instructions.

1.3 REPORTING REQUIREMENTS

FOCUS ON: FISMA METRICS AND OMB RISK ASSESSMENTS

FISMA Metrics

Each year, three sets of FISMA metrics are developed and used to evaluate the performance of agency cybersecurity and privacy programs.

1. The FISMA CIO metrics are developed by OMB and DHS in close coordination with members of the CIO and CISO Communities and assess the degree to which agencies have implemented certain cybersecurity-related policies and capabilities. CFO Act agencies report this information on a quarterly basis, and non-CFO Act agencies report this information twice annually.
2. The FISMA Inspector General (IG) metrics are developed by the Council for Inspectors General on Integrity and Efficiency, in collaboration with OMB and DHS, and are used to provide the independent assessment required under FISMA.
3. The FISMA Senior Accountable Official for Privacy (SAOP) metrics are used to assess the maturity of agency privacy programs. Both the FISMA IG and FISMA SAOP metrics are collected on an annual basis and, along with the fourth quarter FISMA CIO metrics, are reported in the Annual FISMA Report.

OMB Risk Assessments

Following the release of EO 13800, OMB was required to conduct an assessment of agency cybersecurity risk management.

OMB designed an assessment using, in part, FISMA CIO and FISMA IG metrics to provide a high-level view of the degree to which agencies were managing their risk as measured by their implementation of various cybersecurity tools. The assessments have been conducted on a quarterly basis since.

The process is being scaled down and IG metrics are being removed as part of a metrics overhaul process initiated by the Report to the President on the Modernization of Federal IT.

CFO Act agencies can still expect quarterly Risk Management Assessments and non-CFO Act agencies can still expect twice annual assessments.

[16] US-CERT Federal Incident Notification Guidelines. Pg. 1. https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

1.3 REPORTING REQUIREMENTS

OTHER REPORTING

- **Breach Reporting** – OMB requires agencies to report all privacy incidents to the US-CERT within **one hour** of discovering the incident. This requirement applies to "information security incidents, where the confidentiality, integrity, or availability of a Federal information system of a civilian, Executive Branch agency is potentially compromised."[16] The procedures for these reports can be found in the US-CERT Federal Incident Notification Guidelines. The Guidelines are tied to incident reporting and handling guidance in NIST SP 800-61.
- **Major Incident Reporting** – FISMA requires OMB to define a major incident and directs agencies to report major incidents to Congress within **7 days** of identification, and then supplement their initial notification to Congress with a report no later than **30 days** after the agency discovers the breach. Agencies should comply with the criteria set out in the most recent OMB guidance, M-18-02, when determining whether an incident should be designated as major.

DEFINITIONS: BREACH VS. MAJOR INCIDENT

A **breach** is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII, or (2) an authorized user accesses PII for an unauthorized purpose.

A **major incident** is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, the economy of the United States; or to the public confidence, civil liberties, or public health and safety of the American people.

While agencies should assess each breach on a case-by-case basis to determine whether it meets the definition of a major incident, an unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII automatically constitutes a major incident.

Pursuant to PPD-41, if an incident is a major incident, it is also a "significant cyber incident". Thus, a major incident as defined above will also trigger the coordination mechanisms outlined in PPD-41 and potentially require participation and actions from a Cyber Unified Coordination Group.

To further determine if a breach qualifies as a major incident, agencies should use the existing incident management process established in NIST 800-61 and are encouraged to use the US-CERT National Cybersecurity Incident Scoring System (NCISS).

- **High Value Assets Annual Reporting** – OMB issued M-17-09 to provide government-wide guidance for agencies on identifying, prioritizing, and reporting their high value assets (HVAs). All Federal agencies are responsible for keeping their internal HVA lists up-to-date. All CFO Act agencies are required to report all of their HVAs, including a prioritized top ten list, to DHS on an annual basis.
- **Budget Cycle** – As agencies put together their budgets, the CISO is responsible for processing and submitting requests for funding and other budget-related materials for information security. Federal agencies submit initial budget requests to OMB for review in the early fall, often in September, with the President's final budget being due by early February. Agencies must be prepared for the OMB "passback" process if any

[16] The Federal Cybersecurity Workforce Assessment Act is contained in the Consolidated Appropriations Act of 2016 (Public Law 114-113) *See* pages 735-737 at https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

part of their budget needs clarification or revision after its initial submission. OMB issues detailed annual budget guidance to agencies in the form of Circular A-11 and accompanying memos, and agencies have internal policies that detail how exactly their budget is developed and what constraints are put on CISOs in their requests. Because budgets must be planned two years in advance, CISOs must be aware of new guidance and be prepared to justify budgetary decisions and plans.

- **GAO Reporting** – The GAO conducts regular assessments of agencies' information security programs. This reporting is usually tied to specific requests from Congress. GAO may also request materials collected by Inspectors General to produce their reports.
- **Workforce reporting** – As part of the ongoing implementation of the Federal Cybersecurity Workforce Assessment Act[17], agencies reported their work roles of critical need to the Office of Personnel Management (OPM) by April 2018. OPM has issued regular guidance and updated implementation timelines during this process.
- **Quarterly IDC reporting** – Agencies are required to submit specific data to OMB in quarterly Integrated Data Collections (IDCs). These are used to keep track of the agency progress on implementation of initiatives as well as general data about the state of agency cybersecurity programs. The most recent IDC requirements can be found on MAX.

MANAGING YOUR RISK ACROSS THE ENTERPRISE

SECTION 2

2 MANAGING YOUR RISK ACROSS THE ENTERPRISE

INTRODUCTION

Managing Federal cybersecurity is a multi-faceted challenge. CISOs must align their organizations' cybersecurity programs with an ever-changing set of government-wide policies, requirements, and standards. In this section, the challenge is broken down into two parts: managing risk across the enterprise and government-wide policies and initiatives. In practice, these parts are not distinct or partitioned. Government-wide policies create requirements that must be folded into larger risk management approaches, while changing priorities or threat environments within organizations can inform government-wide policy decisions. Managing risk with one eye on the shifting Federal cybersecurity landscape is the central challenge a CISO must face.

Section 2.1 begins with high-level summaries of key risk management reference publications. The CISO should leverage these publications when assessing and improving their organization's cybersecurity posture.

Section 2.2 focuses on a key tool for cybersecurity risk management: The Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework or CSF). The CSF can be a key part of an organization's systematic process for identifying, assessing, and managing cybersecurity risk. It can also serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

The CSF's core functions are summarized in section 2.2, but they warrant brief attention here. The five functions (Identify, Protect, Detect, Respond, Recover) aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. These core functions have been incorporated into recent iterations of the CIO FISMA metrics.

Section 2.3 begins with key government-wide reference policies and memos. These documents collect many of the key information security requirements with which Federal agencies must comply.

Section 2.4 uses a selection of government-wide policies and initiatives to demonstrate how the Federal Government approaches cybersecurity. CISOs must be aware of how their cybersecurity programs are impacted by new requirements in Presidential Directives, OMB memos, BODs, and other documents.

2 MANAGING YOUR RISK ACROSS THE ENTERPRISE

The Cybersecurity Challenge: Part 1

The first challenge a CISO faces when implementing Federal cybersecurity is learning their organization's systems and how to manage resources to keep information secure. The CISO must learn what type of data the public has entrusted to the agency, what level of security is required for each system that stores that data, who can access it, and what should be done if it is breached or otherwise disrupted.

NIST, with considerable input from the private sector, has produced a number of publications to help organizations manage risk. The publications provide guidance to agencies to help them keep track of the many moving parts in their cybersecurity programs and prioritize actions to be taken to improve and maintain their agency's cybersecurity posture.

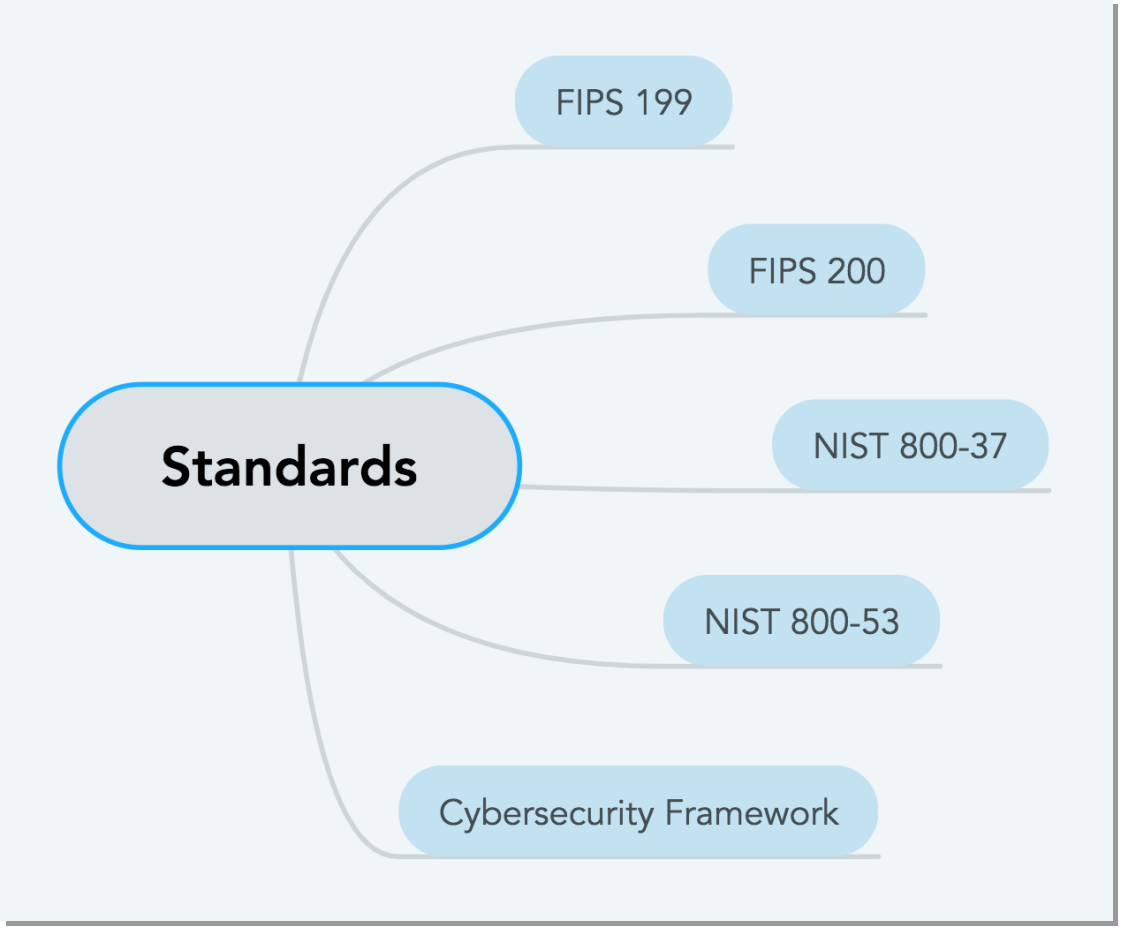
However, NIST publications and risk management processes must be implemented alongside changing government-wide requirements and initiatives, as discussed starting in Section 2.3.

2.1 CISO REFERENCE SECTION: FEDERAL RISK MANAGEMENT

The following are high-level summaries of foundational risk management reference publications. The CISO should leverage these publications when assessing and improving their organization's cybersecurity risk posture. Federal risk management, as defined by NIST, is implemented in partnership with DHS. It is overseen at the agency level by the OIG, and at the Federal level by OMB.

As government-wide authorities issue new policies, updates are made to these documents (or to the guidance supporting them) to provide consistency across the Federal Government. A more comprehensive list of policies related to cybersecurity can be found in the Section A.2 of the appendices.

Government-wide Policies for Section 2.3



2.1 CISO REFERENCE SECTION: FEDERAL RISK MANAGEMENT

FIPS 199 – Standards for Security Categorization of Federal Information and Information System

- Mandates that all Federal information and information systems be given a security categorization to be used in conjunction with vulnerability and threat information when assessing the risk to an organization or system. The security categorization of an information system is determined through an analysis of the types of information residing on that system.
- FIPS 199 also defines three potential impact levels on an organization or individual should there be a breach of security: loss of confidentiality, integrity, or availability. The application of these definitions must take place both within the context of each organization and of the overall national interest. The document explains the relationship between potential impact levels, information types,[18] and security categorization.
- The standards also promote consistent reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.[19]

FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems

Information Systems

- Mandates minimum security requirements for information and information systems supporting the executive agencies of the Federal Government.
- Mandates a risk-based process for selecting the baseline security controls necessary to satisfy the minimum security requirements which agencies tailor to their environment.[20]
- Ties FIPS 199 to supporting NIST special publications to create a risk management program that CISOs can leverage in a consistent and comprehensive manner across agencies.

NIST 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems

- Provides guidance for applying the Risk Management Framework (RMF; *see* Figure 1) to Federal information systems. The six steps of the RMF are: 1) security categorization (FIPS 199), 2) security control selection (NIST SP 800-53), 3) security control implementation, 4) security control assessment, 5) information system authorization, and 6) security control monitoring. The RMF forms the risk lifecycle for Federal information systems from concept to retirement.
- Applying the RMF within enterprises links risk management processes at the information system level to those at the organization level through a risk executive function and establishes lines of responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).[21]

[18] *See* NIST 800-60 Vol 1 – Guide for Mapping Types of Information and Information Systems to Security Categories https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf and Vol 2 – https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

[19] FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[20] FIPS PUB 200 – Minimum Security Requirements for Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[21] NIST Special Publication 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems. Pg. 4. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

2.1 CISO REFERENCE SECTION: FEDERAL RISK MANAGEMENT

NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations

- Provides a catalog of potential security and privacy controls for Federal information systems. The controls address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
- Describes how to develop specialized sets of controls, or overlays, tailored for an organization's specific needs. The consolidated catalog of controls addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms) and an assurance perspective (i.e., the measure of confidence in the security or privacy capability).[23] Controls are meant to be applied within the context of an organization and provide a means to document deviations from Federal baselines.
- Controls also map to the NIST Cybersecurity Framework (discussed in detail in Section 2.2).

[22] Computer Security Resource Center – Risk Management
https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides

2.1 CISO REFERENCE SECTION: FEDERAL RISK MANAGEMENT

Figure 2: Six steps of the Risk Management Framework[22]

[22]Computer Security Resource Center – Risk Management https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides

[23]NIST Special Publication 800-53 – Security and Privacy Controls for Information Systems and Organizations, Revision 5. Pg. 4. https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Managing Risk with the CSF

The Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework or CSF) is a tool originally developed for the private sector that agencies must implement to manage cybersecurity risk in accordance with Executive Order 13800.[24] The CSF can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

An organization can use the CSF as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. It can help an organization determine which activities are most important to critical service delivery, prioritize expenditures, and maximize the impact of investment. The CSF is designed to complement existing business and cybersecurity operations. It provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The CSF consists of three parts: the CSF Core, the CSF Profile, and the CSF Implementation Tiers. The CSF Core (discussed in detail below) is a set of cybersecurity activities, outcomes, and informative references that are common across organizations, providing detailed guidance for developing individual organizational profiles. CSF Profiles help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The CSF Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

Implementation of the CSF[25] involves aligning organization-specific information with the functions, categories, and subcategories detailed in the CSF Core (illustrated in Figure 3 and described below). Figure 4 describes a common flow of information and decisions at the executive, business/process, and implementation/operations levels within an organization.

OMB and DHS have organized the CIO FISMA metrics around the Cybersecurity Framework, leveraging it as a standard for managing and reducing cybersecurity risks and using the core functions to organize the information agencies must submit.

[24] Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure states: "Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk."

[25] NISTIR 8170 – The Cybersecurity Framework: Implementation Guidance for Federal Agencies provides detailed guidance, use cases, and supplementary information to help agencies use the CSF. https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

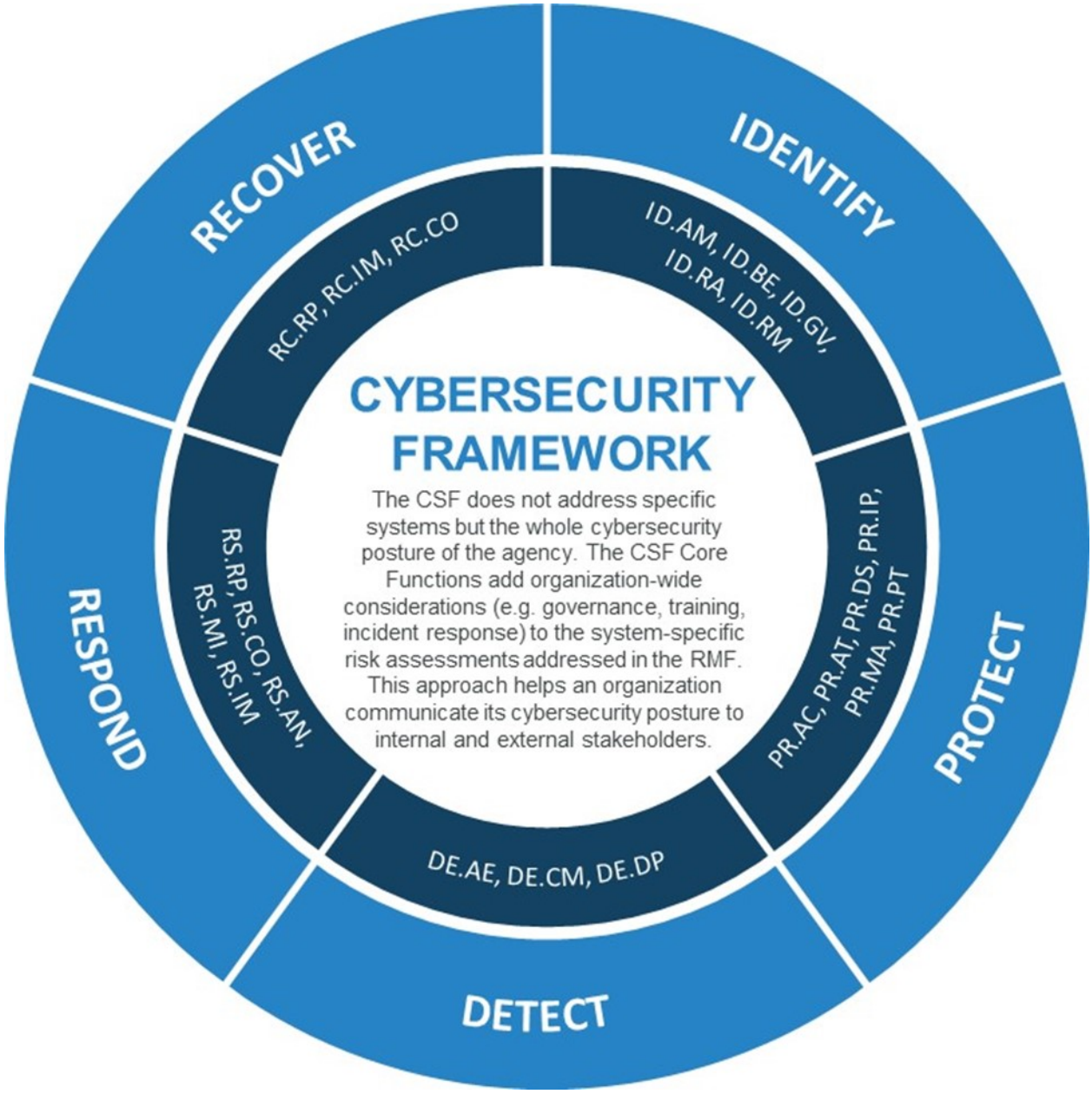


Figure 3: Cybersecurity Framework functions and category unique identifiers[26]

[26]NIST – Cybersecurity Framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

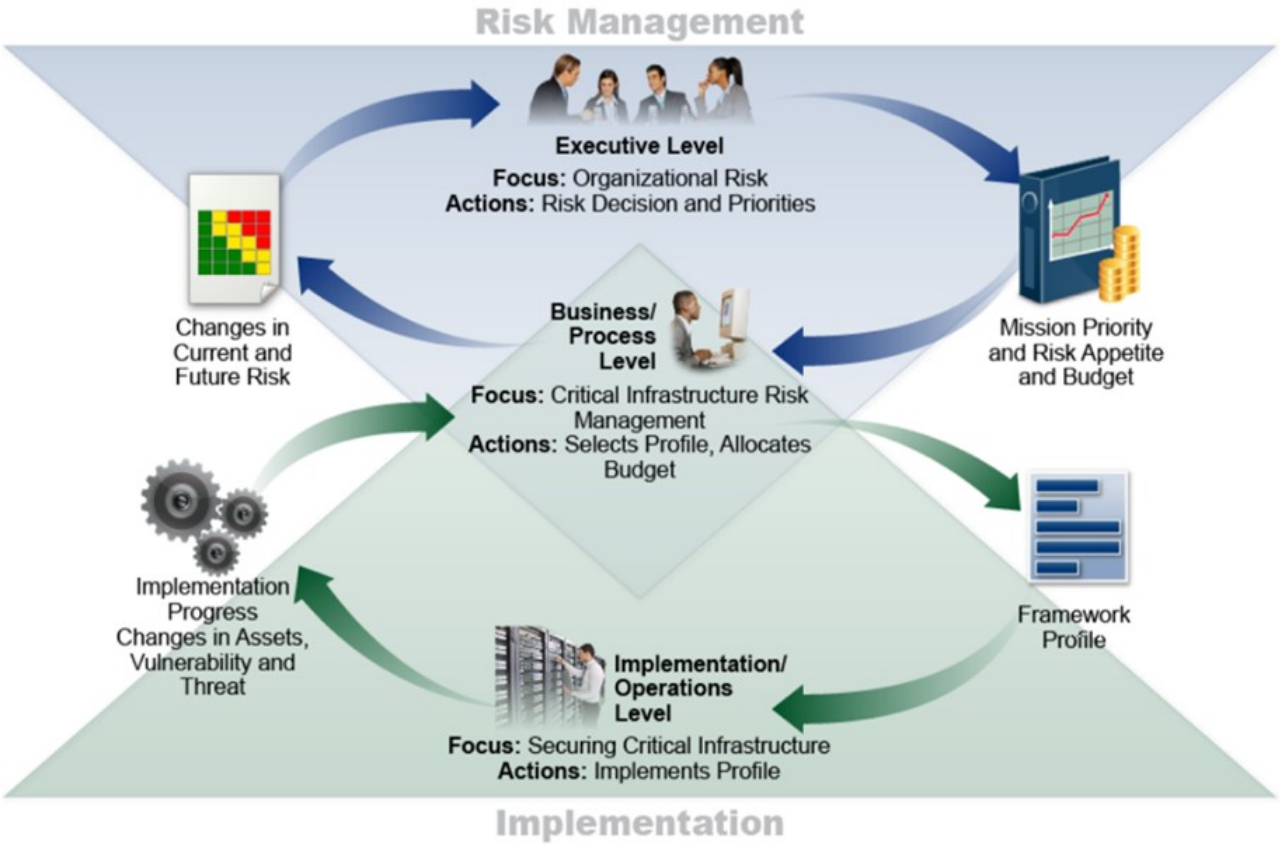


Figure 4: Notional Information and Decision Flows within an Organization[27]

As a whole, the CSF consolidates multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry. What the CSF does not provide is an organizational change process. It is a model from which change can be tailored and implemented, but it does not tell organizations what specific actions must be taken to enact that change.[28]

[27] Framework for Improving Critical Infrastructure Cybersecurity. Pg. 12. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[28] Framework for Improving Critical Infrastructure Cybersecurity. Pg. 1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

The CSF Core

The CSF Core is divided into five functions which aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and learning from previous activities. The five functions and their basic objectives are:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Each of the five functions are divided into categories which are accompanied by broad objectives. The categories are then divided into subcategories with more specific objectives. Agencies must determine whether or to what extent these objectives have been met and prioritize their actions accordingly.

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

The actual security operations involved in meeting the objectives in the CSF will differ from agency to agency. Because every agency must analyze its own systems and incorporate its own organizational priorities, there is no one-size-fits-all process for risk management.

In the following highlights, each CSF Core function will be matched with internal agency policies. The goal of this is to show how internal policies can be designed to achieve specific objectives at the subcategory level of the CSF Core. While creating policy and operationally achieving outcomes are different things, a CISO can examine the policies that exist within their organization to assess strengths and recognize gaps.

NOTE: The internal agency policies used as examples in this section are purely illustrative and should not be copied wholesale by organizations in place of detailed risk analysis. They are included to give new CISOs a starting point from which to develop policy from scratch when appropriate, tailored to their organization's needs.

The activities described in the highlights below are complex and different for each organization. Having directives in place is only the beginning of the actual work of cybersecurity management.

NIST 800-53 controls, to which the CSF is tied, are used during Office of the Inspector General audits mandated by FISMA. The controls and how to assign them to systems is discussed in detail in NIST 800-53 and reinforced as a step in the Risk Management Framework process.

However, having policies in place that address controls (and satisfy high-level audits) is only effective if the required resources are in place for those controls to be executed. Ultimately, risk management is about ensuring resources can be used effectively in accordance with policy, not just that policy is in place.

[29]Framework for Improving Critical Infrastructure Cybersecurity. Pg. 19. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Identify (ID) Function Highlights

The activities in the Identify function are foundational for effective use of the CSF. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Categories within this function include: Asset Management (highlighted below); Business Environment; Governance; Risk Assessment (highlighted below); and Risk Management Strategy.

The categories highlighted below demonstrate the connections from example agency policies to the NIST 800-53 controls they implement to the CSF Functions, Categories, and Subcategories they satisfy for the purposes of assessing risk.

NOTE: These are only highlights. They do not imply that these categories are more important than the others or that the example agency's policies represent a transferrable or paradigmatic approach to risk management.

ASSET MANAGEMENT (ID.AM)

ID.AM Desired Outcome: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.[30]

The subcategories within ID.AM provide more specific objectives. Subcategories ID.AM-1 and ID.AM-2 are about inventorying the "physical devices and systems" and the "software platforms and applications" within the organization, respectively. The example agency's Secure Asset Management Policy assigns the maintenance of an enterprise-wide inventory of components on the network infrastructure to infrastructure managers. The specific controls involved in this process are tied to NIST 800-53 (in this case, the control code is CM-8). It is important to note that the example agency policy does not mention the ID.AM categorization because the actual control in use appears in NIST 800-53. In the context of a risk assessment of its cybersecurity program, however, the example agency meets the objectives of the ID.AM-1 and ID.AM-2 subcategories at the policy level.

[30] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

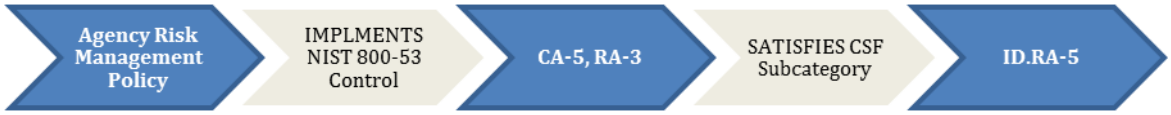
[31] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

RISK ASSESSMENT (ID.RA)

ID.RA Desired Outcome: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.[31]

The subcategories within ID.RA provide specific objectives that encourage agencies to use "threats, vulnerabilities, likelihoods, and impacts" to determine risk (subcategory ID.RA-5). The example agency's Risk Management Policy directs Information System Security Officers (ISSOs) to conduct risk assessments on "all identified weaknesses" with the help of updated content on those weaknesses provided by System Owners (SOs). These actions are tied to each system's Plan of Action & Milestones (POA&M) as noted in NIST 800-53 control CA-5. The Risk Assessment requirement is also tied to NIST 800-53's controls, in this case RA-3 and several others. The example agency meets the objectives of the ID.RA-5 (and the other subcategories within the Risk Assessment and Risk Management categories) at the policy level by having a risk assessment procedure in place.



It is no accident that the CSF includes risk assessment and risk management as desired outcomes within the Identify function, reinforcing the fact that the activities found under Identify provide the foundation for the other CSF functions.

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Protect (PR) Function Highlights

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

Categories within this function include: Access Control (highlighted below); Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance (highlighted below); and Protective Technology.

The categories highlighted below demonstrate the connections from the example agency's policies to the NIST 800-53 controls they implement to the CSF Functions, Categories, and Subcategories they satisfy for the purposes of assessing risk.

NOTE: These are only highlights. They do not imply that these categories are more important than the others or that the example agency's policies represent a transferrable or paradigmatic approach to risk management.

IDENTITY MANAGEMENT AND ACCESS CONTROL (PR.AC)

PR.AC Desired Outcome: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.[32]

The subcategories within PR.AC provide more specific objectives. The example agency's Access Control Policy assigns responsibility for controls in NIST 800-53 to various managers, supervisors, and SOs in accordance with their positions and the network components they oversee. Each of the roles is tied directly to a NIST control (from AC-2 to AC-21) covering many of the Access Control objectives under the Protect function of the CSF. Subcategory PR.AC-3 ("Remote access is managed"), for example, is assigned to SOs and tied to NIST control AC-17. Because responsibility for these objectives is clearly delegated in policy, the example agency has met the objective for that subcategory at the policy level.

MAINTENANCE (PR.MA)

PR.MA Desired Outcome: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.[33]

The subcategories within PR.MA provide more specific objectives. The first of those objectives, PR.MA-1, asks agencies to assess whether "maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools." The example agency's System Maintenance Policy requires that account

[32] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP NIST.CSWP.04162018.pdf

[33] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/ NIST.CSWP.04162018.pdf

Protect (PR) Function Highlights

managers and SOs have their maintenance responsibilities laid out in policy and connected to government-wide controls. NIST 800-53 lays out update schedules for updating system maintenance policy and procedures (MA-1) and actually performing system maintenance (MA-2 and MA-3). The example agency's policy ties to these controls, which means that potential risk from improper or incomplete system maintenance has been managed. However, just like the Access Control Policy above, this policy must be reviewed regularly to ensure that new systems and personnel are incorporated and aware of their responsibilities.

Given that systems and personnel are constantly changing, policies must be reviewed regularly to ensure that sufficient resources are being devoted to the Protect function's objectives. Agencies should reassess risks when major system changes are made or when new personnel are brought in, which is why training is also a key component of the Protect function.

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Detect (DE) Function Highlights

The Detect function enables timely discovery of cybersecurity events.

Categories within this function include: Anomalies and Events; Security Continuous Monitoring (highlighted below); and Detection Processes.

The categories highlighted below demonstrate the connections from the example agency's policies to the NIST 800-53 controls they implement to the CSF Functions, Categories, and Subcategories they satisfy for the purposes of assessing risk.

NOTE: These are only highlights. They do not imply that these categories are more important than the others or that the example agency's policies represent a transferrable or paradigmatic approach to risk management.

SECURITY CONTINUOUS MONITORING (DE.CM) - CM POLICY AND MALICIOUS CODE

DE.CM Desired Outcome: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.[34]

For the subcategories within DE.CM, two different example agency policies can be used to demonstrate approaches to general and specific threats, respectively. First, the example agency's Continuous Monitoring Policy fulfills the objectives in subcategory DE.CM-1 ("the network is monitored to detect potential cybersecurity events"). It also fulfills objectives in the subcategory for Detection Processes, DE.DP-1 ("roles and responsibilities for detection are well defined to ensure accountability"). These objectives connect to government-wide policies that require each agency to have a CM strategy in place as well as NIST 800-53 controls (CA-7 for CM and AR-4 for Privacy).

Second, the example agency has a policy specifically for Malicious Code that assigns scanning responsibilities to its Security Operations Center (SOC). Not every agency has a partitioned SOC, so this kind of policy must be tailored to reflect the lines of authority within each agency. In the example agency's case, the policy fulfills DE.CM-4.("malicious code is detected") by tying to the NIST 800-53 controls that address this type of threat (SI-3, SI-8, and SI-16).

[34] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Detect (DE) Function Highlights

Detection processes must constantly evolve with the threat landscape, and this means that new government-wide initiatives can necessitate updates to CM policy. The need to regularly review internal CM policies and strategy reinforces the ongoing nature the Detect function, and of risk management as a whole.

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Respond (RS) Function Highlights

The Respond function supports the ability to contain the impact of a potential cybersecurity event.

Categories within this function include: Response Planning; Communications (highlighted below); Analysis; Mitigation; and Improvements.

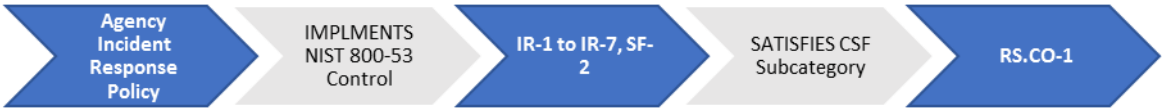
The categories highlighted below demonstrate the connections from the example agency's policies to the NIST 800-53 controls they implement to the CSF Functions, Categories, and Subcategories they satisfy for the purposes of assessing risk.

NOTE: These are only highlights. They do not imply that these categories are more important than the others or that the example agency's policies represent a transferrable or paradigmatic approach to risk management.

COMMUNICATIONS (RS.CO)

RS.CO Desired Outcome: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.[35]

The subcategories within RS.CO provide more specific objectives. The first of those objectives, RS.CO-1, asks agencies to assess whether "[p]personnel know their roles and order of operations when a response is needed." The example agency's Incident Response Policy assigns all agency personnel the responsibility to report suspected incidents to the agency's SOC. It then details actions that must be taken by the SOC and other personnel to respond to the potential threat. As with the policies discussed above, the agency ties its procedures to controls in NIST 800-53, which recommend regular updates to incident response policies. The controls include IR-1 through IR-7 for policy, procedure, and reporting. Also included is the control SE-2 for actions related to privacy. In the case of incident response, agencies must also have a process for reporting to government-wide authorities like US-CERT.



The Respond function is not just about demonstrating that during-incident responsibilities are assigned on paper, it is about knowing that the proper execution of incident response can be anticipated and expected. Government-wide authorities are set up to help agencies review their actions during an incident, both in the interest of the agency itself and the larger Federal cybersecurity landscape.

[35] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

Recover (RC) Function Highlights

The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

Categories within this function include: Recovery Planning (highlighted below); Improvements; and Communications.

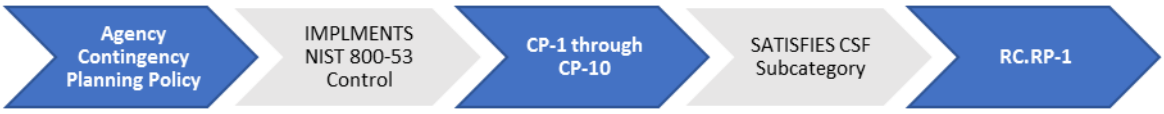
The categories highlighted below demonstrate the connections from the example agency's policies to the NIST 800-53 controls they implement to the CSF Functions, Categories, and Subcategories they satisfy for the purposes of assessing risk.

NOTE: These are only highlights. They do not imply that these categories are more important than the others or that the example agency's policies represent a transferrable or paradigmatic approach to risk management.

RECOVERY PLANNING (RC.RP)

RC.RP Desired Outcome: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.[36]

The subcategories within RC.RP provide more specific objectives. Subcategory RC.RP-1 asks agencies to ensure that their "[r]recovery plan is executed during or after an event." The example agency's Contingency Planning Policy sets expectations for Infrastructure Managers and SOs to conduct Disaster Recovery (DR) tests, Business Impact Analyses (BIAs), and Contingency Plan (CP) testing for components under their control. These actions are tied to NIST 800-53 controls for Contingency Planning, specifically CP-1 through CP-10.



Risk management is not effective unless it is taking all systems and components into account. This means that a CISO must understand the potential impact of damage to any of these components and ensure personnel are aware of their roles to mitigate damage if an incident does occur. The Recover function can help increase awareness of potential impact from the SO level all the way up to the executive level. Therefore, Recover must be constantly considered in conjunction with all the other functions, not just once a threat is identified.

[35] Framework for Improving Critical Infrastructure Cybersecurity. Table 2: Framework Core. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.2 THE NIST CYBERSECURITY FRAMEWORK AT A GLANCE

CSF Core: Takeaways

- The CSF Core can help an agency determine which steps would improve their cybersecurity posture, and in what order.
- The cybersecurity activities, outcomes, and informative references laid out in the Core functions are common across organizations, but the CSF is a tailorable model for organizational change, not a change process in itself.
- The next step after comparing their policies against NIST 800-53 controls and CSF desired outcomes is for agencies to use the other resources in this handbook and the tools and services offered by government-wide organizations to constantly improve their cybersecurity posture.
- Success will not look identical for each organization, so CISOs must determine what actions would make their organization's information appropriately secure.

2 MANAGING YOUR RISK ACROSS THE ENTERPRISE

The Cybersecurity Challenge: Part 2

Several times in Sections 2.1 and 2.2, risk management is referred to as an "ongoing" endeavor. This is due to the cybersecurity landscape constantly changing and, therefore, the comprehensive list of related government-wide requirements constantly changing with it.

A challenge every organization faces is that as these comprehensive requirements change, they must be mapped to existing internal agency policies to identify the gaps in the organization's cybersecurity posture and then update those policies as appropriate.

New threats can result in requirements that cause agencies to shift resources, creating vulnerabilities. New reporting requirements can draw personnel away from other cybersecurity tasks. New initiatives can change organizational priorities and render previous risk assessments outdated. Managing risk with one eye on the shifting Federal cybersecurity landscape is the central challenge a CISO must face.

2.3 CISO REFERENCE SECTION: GOVERNMENT-WIDE REQUIREMENTS

The following is a list of key government-wide reference policies and memos. These documents collect many of the key information security requirements with which Federal agencies must comply.

A more comprehensive list of policies related to cybersecurity can be found in the Section A.2 of the appendices. Additional policies and related resources can be found on OMB.gov and DHS.gov.

Government-wide Policies for Section 2.3

OMB Circular A-130 – Managing Information as a Strategic Resource

- Establishes general policy for Federal information technology. The policy section of the document lays out agency responsibilities for major areas of IT and establishes government-wide responsibilities for key organizations.
- Appendices include responsibilities for protecting Federal information resources and managing personally identifiable information (PII).
- Useful as a consolidated list of requirements and policies for reference but does not necessarily contain all requirements related to any given IT area. Agencies are responsible for implementing the requirements in the Circular and those in other OMB policies and guidance in a mutually consistent fashion.[37]

2.3 CISO REFERENCE SECTION: GOVERNMENT-WIDE REQUIREMENTS

Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- Directs agencies to implement The Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework or CSF).

OMB M-18-02 – Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements

- Contains the most recent FISMA reporting guidance and deadlines. It describes the processes for Federal agencies to report to OMB and, where applicable, DHS.
- Each fiscal year, OMB releases a similar memo that establishes new requirements and consolidates requirements from prior OMB annual FISMA guidance to ensure consistent, government-wide performance and agency adoption of best practices.[38]

OMB M-17-25 – Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- Provides implementing guidance for actions required in Executive Order 13800.
- Requires agencies to create an action plan for implementing the CSF.[39]
- Appendices lay out risk assessment procedures and summarize CSF's Core functions.

OMB M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information

- Sets forth policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII).
- Includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach.
- Provides guidance on whether and how to provide notification and services to affected individuals.

OMB M-17-09 – Management of Federal High Value Assets[40]

- Provides government-wide guidance for agencies on identifying, prioritizing, and reporting their high value assets (HVAs).
- All Federal agencies are responsible for keeping their internal HVA lists up-to-date. All CFO Act agencies are required to report all of their HVAs, including a prioritized top ten list, to DHS on an annual basis.

OMB M-14-03 – Enhancing the Security of Federal Information and Information Systems

- Establishes requirements and outlines specific actions for agencies to follow in establishing information security

[37]Circular A-130 – Managing Information as a Strategic Resource. Pg. 2. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars A130/a130revised.pdf

[38]M-18-02 – Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements. Pg. 1. https:/ www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf

[39]Agency action plans for CSF implementation were due July 14, 2017.

[40]This policy is expected to be updated in Summer 2018.

continuous monitoring (ISCM) programs.

- Issued as part of coordinated government-wide CDM program at DHS.
- Ties guidance to NIST 800-37, NIST 800-137, and NIST 800-53.

OMB M-08-23 – Securing the Federal Government's Domain Name System Infrastructure

- Establishes policies for deploying Domain Name System Security (DNSSEC) to all Federal information systems.

PPD-41 – Presidential Policy Directive – United States Cyber Incident Coordination

- Sets forth principles governing the Federal Government's response to any cyber incident, whether involving public or private sector entities.
- Establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response for significant cyber incidents.
- Requires the Department of Justice (DOJ) and DHS to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.

The US-CERT Federal Incident Notification Guidelines

- Contains the procedures for reporting Privacy Incidents to US-CERT.
- The Guidelines are tied to incident reporting and handling guidance in NIST SP 800-61. The definitions and procedures for major incidents can be found in M-18-02.

2.4 GOVERNMENT-WIDE INITIATIVES

The following is a selection of policies and initiatives that demonstrate how the Federal Government approaches cybersecurity. CISOs must be aware of how their cybersecurity programs are impacted by new and existing requirements in Presidential Directives, OMB memos, BODs, and other documents.

Examples of Government-wide Initiatives

Continuous Diagnostics Mitigation (CDM)

The CDM program, developed at DHS, "provides a consistent, government-wide set of information security continuous monitoring (ISCM) tools to enhance the Federal Government's [sic] ability to identify and respond, in real-time or near real-time, to the risk of emerging cyber threats."[41]

As Figure 5 illustrates, agency-installed sensors are deployed to perform an on-going, automated search for known cyber flaws. Results from the sensors feed into an agency dashboard that produces customized reports that alert network managers to their most critical cyber risks. Prioritized alerts enable agencies to efficiently allocate resources based on the severity of the risk. Progress reports track results, which can be used to compare security postures among agency networks. Summary information feeds into a Federal enterprise-level dashboard to inform and provide situational awareness into the cybersecurity risk posture across the Federal Government.

Figure 5: CDM Process[42]

[41]M-14-03: Enhancing the Security of Federal Information and Information Systems. Pg. 2. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

[42]Continuous Diagnostics and Mitigation https://www.dhs.gov/cdm

2.4 GOVERNMENT-WIDE INITIATIVES

Continuous Diagnostics Mitigation (CDM) (CONT)

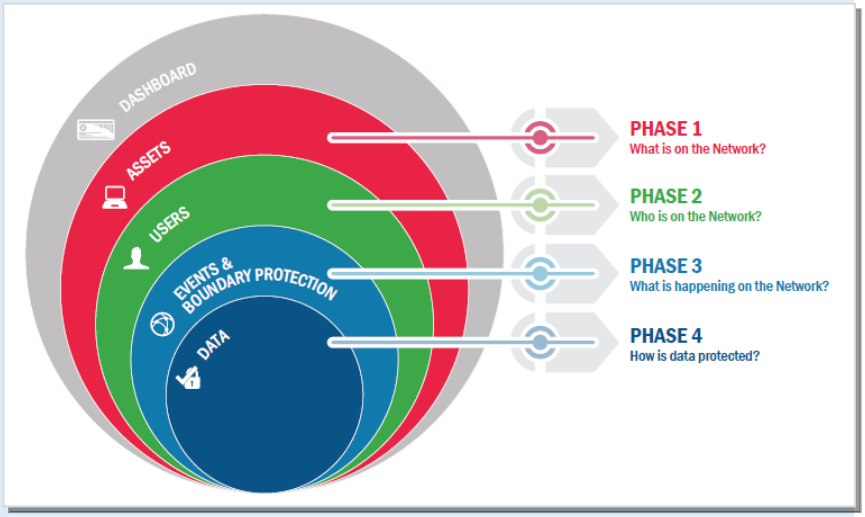
DHS and GSA work together to help agencies with the acquisition of CDM tools even as those tools evolve and present opportunities for improvement. The CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) contract is the next step in the evolution of CDM toward ongoing authorization and cloud security. CDM DEFEND supports the transformation of the system authorization process by developing and implementing more efficient ongoing assessment and authorization across the Federal enterprise. The new contract is anticipated to support, among other activities, enhanced cloud and mobile cybersecurity, a more standardized approach for incident response across the Federal enterprise environment, and more robust boundary protections aligned with the ongoing IT modernization efforts.

Government-wide service offerings like CDM are often tied to larger Federal cybersecurity strategies and initiatives. To fully implement the CDM program and create consistent government-wide ISCM approach, OMB issued M-14-03. The memo required agencies to develop a ISCM strategy according to specific government-wide standards and included a detailed list of actions agencies had to take within established timelines. The memo's requirements are tied to existing NIST publications, including ones that are included in the "Informative References" section of the CSF Core.

2.4 GOVERNMENT-WIDE INITIATIVES

Focus On: CDM Phases

The CDM program is organized by phases, as identified in the diagram shown here and described below.



Phase 1: "What is on the network?"
Managing "what is on the network?" requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

Phase 2: "Who is on the network?"
Managing "who is on the network?" requires the management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE). These four functions have significant interdependence and are thus managed together as part of Phase 2.

Phase 3: "What is happening on the network?"
Managing "what is happening on the network?" builds on the CDM capabilities provided by "what is on the network?" and "who is on the network?" These CDM capabilities include network and perimeter components, host, and device components, data at rest and in transit, and user behavior and activities. These capabilities move beyond asset management to more extensive and dynamic monitoring of security controls. This includes preparing for and responding to behavior incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure.

Phase 4: "How is data protected?"
CDM Phase 4 capabilities support the overall CDM program goal to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

CDM Agency and Federal Dashboards
At the agency level, security staff will be able to identify, analyze, and address priority vulnerabilities. Summary data from each participating agency's dashboard will be transmitted to the Federal Dashboard where the tactical data will be used to inform strategic decision making regarding systemic cybersecurity risks across the entire Federal civilian enterprise.

2.4 GOVERNMENT-WIDE INITIATIVES

High Value Assets (HVAs)

OMB-issued policies are the most common way that changes to government-wide requirements are disseminated to agencies. As the threat environment and the Federal computing landscape evolve, policies must be updated to ensure that assets are protected in a way that is commensurate with their importance. OMB issued M-17-09, to update definitions and guidance for HVAs. Memos of this type often contain both policy (mandatory requirements, roles and responsibilities for key organizations, lines of authority) and guidance (approaches for implementation). In the case of this HVA memo, the guidance must be followed in order to properly identify HVAs (effectively making the guidance mandatory). However, in some cases the guidance is broader and merely suggests actions.

While government-wide policies like this one are not directly tied to the CSF in the same manner as NIST publications, the requirements in these policies and the minimum security requirements in FIPS publications are designed to be mutually compatible. The HVA memo lists FIPS publications and other authorities that must be taken into account during implementation. NIST publications are updated regularly to account for newly issued government-wide policies.

Takeaways:

- Risk for all systems is not equal, and agencies must know which of their assets require specialized protection.
- Agencies must take a strategic enterprise-wide view of risk that accounts for all critical business and mission functions when identifying HVAs.
- Agencies must also establish appropriate governance of HVA activities across the enterprise and should integrate HVA remediation activities into agency planning, programming, budgeting, and execution processes.
- Agencies must develop, maintain, and regularly update their HVA inventory lists, at least annually.

Figure 6: Agency HVA Process Framework[43]

[43] M-17-09 – Management of Federal High Value Assets https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf

2.4 GOVERNMENT-WIDE INITIATIVES

Breach of Personally Identifiable Information (PII)

When a breach occurs, the kind of information breached often determines the nature of the response. PII contained on government servers must be treated differently than other kinds of information because it is entrusted to cybersecurity officials on the public's behalf. The Privacy Act and other authorities protect users of Federal services from unauthorized access to their information.

OMB issued M-17-12 to clarify the specific actions required by agencies when responding to a breach of PII. The memo "reflects certain changes to laws, policies, and best practices that have emerged since the [OMB] first required agencies to develop plans to respond to a breach."[44] The issuance of such policies necessitate changes in the corresponding internal policies for each agency (in this case to their breach response procedures and the related reporting requirements, which are tied to NIST publications and DHS reporting policies, respectively).

Takeaways:

- Breaches involving PII trigger a set of required actions in addition to usual breach procedures.
- Specific actions must be taken by the agency's Senior Agency Official for Privacy (SAOP), who works closely with the CIO and CISO during privacy-related incidents.

Binding Operational Directives (BODs)

In coordination with OMB, DHS develops and oversees implementation of Binding Operational Directives (BODs) "for purposes of safeguarding Federal [sic] information and information systems."[45] Federal agencies are required to comply with these policies, which often come with background information and action plans attached. BOD-18-01 mandates specific security standards to promote "cyber hygiene." It lays out required actions for agencies to enhance email and web security.

BODs are also used to respond to specific government-wide threats, as in the case of BOD-17-01. This BOD was issued when it became clear that Federal hardware from Kaspersky may have been compromised. Agencies were asked to make a plan to discontinue use of the potentially unsecured products.

Takeaways:

- BODs are a form of government-wide response to cybersecurity issues targeted at government-wide action.
- Agencies are required to comply with BODs.
- BODs can be issued in response to specific threats or can mandate government-wide changes.

[44] M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information. Pg. 1. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[45] BOD-18-01: Enhance Email and Web Security https://cyber.dhs.gov/assets/report/bod-18-01.pdf

2.4 GOVERNMENT-WIDE INITIATIVES

NIST National Cybersecurity Center of Excellence: Data Integrity Attacks

While some policy develops from administration initiatives or specific known cybersecurity threats, many government-wide publications come from rigorous, proactive investigation of the threat landscape. The National Cybersecurity Center of Excellence (NCCoE) at NIST aides the development of effective cybersecurity policy by testing methods and techniques in a laboratory environment. In the case of the NIST SP 1800-series, the NCCoE provides practice guides to help agencies test their networks against various threats.

Once such publication, NIST SP 1800-11, allows agencies to test their recovery methods in the case of data integrity attacks. This publication is guidance, so it does not establish any new requirements. Agencies "can choose to adopt [the publication's] solution or one that adheres to these suggested guidelines," or they can "use [the] guide as a starting point for tailoring and implementing parts of the solution."[46] While adopting minimum security requirements from documents like FIPS 200, agencies should be aware of these practice guides and other guidance that NIST provides to strengthen networks across the Federal Government.

Takeaways:

- Policies can be developed through investigation and research, not only through administration initiatives and reactions to threats.
- Government-wide standards and requirements are developed by NIST with considerable private-sector and industry input.
- Awareness of the full range of publications and guidance will help CISOs improve their cybersecurity programs.

[46]NIST SP 1800-11 – Data Integrity: Recovering from Ransomware and Other Destructive Events Pg. 2 https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf

2.4 GOVERNMENT-WIDE INITIATIVES

The Joint Cybersecurity Performance Measurement Working Group: Driving Preferred Outcomes through the Evaluation Process

In addition to providing CIOs, CISOs, and agency leadership with information on the status of their information security programs, the evaluation materials derived from FISMA metrics can be leveraged to drive specific outcomes sought after by the CISO community. The metrics themselves are derived through a collaborative process between members of the OMB- and DHS-led Joint Cybersecurity Performance Measurement Working Group (JCPMWG), a subcommittee of the CISO Council.

Open to members of the Federal CISO Community and their staff, the JCPMWG regularly revisits the FISMA metrics to determine whether they reflect current security needs. Part of this process involves soliciting the priorities CIOs and CISOs wish to drive toward and the advanced capabilities they seek to implement. This allows CISOs to help shape the metrics process to ensure it is helping them achieve their goals and priorities.

The JCPMWG also frequently helps drive prioritization of metrics in various oversight materials. For instance, due in large part to priorities expressed by the JCPMWG and Federal cybersecurity community, anti-phishing capabilities were added in 2015 to the Cybersecurity Cross-Agency Priority (CAP) Goal, which represents the Executive Branch's Federal management priorities. With these security areas elevated in the then-Administration's priorities, CISOs were able to seek greater investment in these capabilities in order to improve their standing in these critical areas. When the anti-phishing targets were added to the CAP goal, only about half of the civilian CFO Act agencies were meeting them. By the time the CAP Goal closed at the end of FY 2017, they were all meeting the targets.

MANAGEMENT RESOURCES

SECTION 3

3 MANAGEMENT RESOURCES

INTRODUCTION

Section 3 is intended to increase a CISOs awareness of resources and processes not covered in the first two sections.

Sections 3.1 and 3.2 provide basic information to help a CISO manage personnel decisions as they work to improve their organization's cybersecurity posture. Current efforts to address workforce challenges in a government-wide manner have led to the development of new tools and services to help organizations establish a better high-level view of their cybersecurity workforce and the gaps therein.

Section 3.3 lists some of the services available through government-wide organizations, especially DHS and GSA. CISOs should be aware of the tools and acquisition vehicles that have been put in place to help organizations navigate cybersecurity challenges. A catalog of GSA services, links, and additional information has been provided in Section A.4 of the appendices.

3.1 WORKFORCE

Cybersecurity workforce management is a responsibility the CISO shares with their agency's Human Resources department and the agency CIO. The Federal Cybersecurity Workforce Assessment Act of 2015 was passed to assess and improve the Federal Government's ability to recruit, hire, and retain cybersecurity talent. The Act's implementation has been a collaborative effort between NIST, OPM, DHS, and Federal agencies, and has bolstered the development of government-wide workforce standards and resources.

Each agency is permitted to create their own process for recruitment and hiring based on their organizational needs. Since managers, HR departments, and organizational stakeholders may interpret hiring needs differently, a CISO must be aware of government-wide standards and their organization's recruitment and hiring processes.

NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, also known as the NICE Framework or NIST SP 800-181, is an important tool for evaluating your organization's cybersecurity workforce, filling vacancies, and creating ongoing plans for employee development. The NICE Framework establishes taxonomy and common lexicon used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The NICE Framework breaks the task of workforce management down into a system of codes which can then be used to make personnel decisions. It is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions;
- Specialty Areas (33) – Distinct areas of cybersecurity work; and
- Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role.
    - ◊ Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.
    - ◊ Tasks – Specific defined pieces of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.

In January 2017, OPM issued government-wide guidance on assigning new cyber codes that are aligned to the NICE Framework. Agencies are working through the process of applying the codes to their cybersecurity workforce, and the next phase of implementation (reports on which were due to OPM by April 2018) will require agencies to identify and report on Work Roles of Critical Need.

3.1 WORKFORCE

THINGS TO KNOW

- **Direct-Hire Authority (DHA)** – an appointing (hiring) authority that the Office of Personnel Management (OPM) can give to Federal agencies for filling vacancies when a critical hiring need or severe shortage of candidates exists. OPM posts a list of the current Government-wide DHAs. In addition, agencies must post all vacancies filled by DHA on USAJOBS.gov. There are two methods under which OPM issues Direct-Hire Authority:
    - ◊ An agency with delegated examining authority may submit a written request to OPM for specific positions; or
    - ◊ OPM may decide independently that a "severe shortage of candidates" or a "critical hiring need" exists for specific positions in some or all locations and issue authority either Government-wide or for specific agencies and/or locations.
    - ◊ **CIO Hiring Authorities** – The recently issued Executive Order Enhancing the Effectiveness of Agency Chief Information Security Officers (EO 13833) directed OPM to establish rules under which they grant DHA for IT positions of critical need.
- **Veterans' Preference** – Under 5 U.S.C. 2108, and supported by implementing regulations by OPM, certain types of active duty service may qualify for veterans' preference (i.e., preference eligible). [47]
- **CIO Council's Workforce Committee** – This group's agenda encompasses the full employment life cycle: workforce planning, recruitment, retention, and career development. The Committee works with the HR community to develop, implement and communicate strategies to recruit, retain, and manage a fully trained and qualified IT workforce, to meet current and future mission requirements. Their Strategic Initiatives include:
    - ◊ Multi-Agency Recruitment and Hiring Events;
    - ◊ IT Track of the President's Management Council Interagency Rotational Program;
    - ◊ Position Description Library; and
    - ◊ Strategic Career Roadmaps.

[47] *See*: Government-wide Veterans Recruitment and Employment Strategic Plan FY2014-FY2017 https:// www.fedshirevets.gov/pdf Vets_Initiative_Strategic_Plan_2014.pdf

See also: Employment of Veterans in the Federal Executive Branch Fiscal Year 2014 https://www.fedshirevets.gov/hire/hrp/reports/ EmploymentOfVets-FY14.pdf

3.1 WORKFORCE

NICCS Workforce Resources

The **National Initiative for Cybersecurity Careers and Studies** is an online resource provided by DHS for cybersecurity training. It connects Government employees, students, educators, and industry with cybersecurity training providers throughout the nation. The NICCS website hosts a variety of resources that can help agencies improve their cybersecurity workforce.

The Explore the Framework Tool is a navigable version of the NICE Framework that lays out its seven categories and their specialty areas. The work roles listed in the NICE Framework are shown with their associated OPM codes alongside resources for training, position descriptions, and other related information. Using the tool, those making cybersecurity personnel decisions can map out their current workforce and identify gaps and needs. It can provide a printable inventory of roles, reporting assistance to help account for full and vacant positions, and graphics that show how much of your workforce is mapped to each of the seven NICE Framework categories.

The NICCS Education and Training Catalog contains over 3,000 cybersecurity and cyber-related courses offered nationwide. The catalog allows agencies to search for courses and training opportunities available to Government workers. Integrated with the Training Catalog is the Federal Virtual Training Environment (FedVTE), which provides free online, on-demand training in cybersecurity for Federal employees and contractors which is aligned to the certifications included in the NICE Framework.

The Cybersecurity Workforce Development Toolkit helps agencies assess and understand their cybersecurity workforce risks. The Toolkit provides templates for workers to create cybersecurity career paths and resources to help agencies recruit and retain top cybersecurity talent. Among its time-saving features is the PushButton PD Tool, which can help an agency build a position description (PD) that is aligned to the NICE Framework. It generates the PD with associated documents, helping both managers and HR departments streamline their recruitment process.

3.2 CONTRACTING

When developing their cybersecurity programs, agencies often turn to private sector companies to perform many necessary tasks and provide critical capabilities. Contracting needs vary widely by agency, with some using hundreds of contractors and some using small teams to supplement their full-time Federal operations staff. Service providers from the private sector are, in many cases, able to leverage the common needs of agencies to provide more efficient and cost-effective products.

CISOs must be aware of the regulations that govern contracting and the wide variety of acquisition vehicles and support services offered, especially by GSA, that are tied to those regulations. GSA makes certain targeted or government-wide contracts available to meet agency demands or to help leverage market forces to provide agencies with products and services that address identified needs. A few key examples are discussed below, and a full list of GSA offerings is included in the Section A.4 of the appendices.

For detailed information and ordering procedures, see "GSA IT Products and Services."

Federal Acquisition Regulation (FAR)

The Federal Acquisition Regulation (FAR) is the set of rules that governs the acquisition process for Federal agencies. It is codified in Title 48, Chapter 1 of the Code of Federal Regulations and empowers agencies to purchase or lease goods and services by contract using appropriated funds. The FAR establishes requirements for acquisition planning, contract formation, and contract administration. CISOs will usually interact with the FAR language indirectly because of the range of services that GSA has provided to make IT services easier to purchase.

GSA Schedules and Contract Types

Under the GSA Schedules Program (also referred to as Multiple Award Schedules and Federal Supply Schedules), GSA establishes long-term government-wide contracts with commercial firms to provide access to over 11 million commercial supplies (products) and services. Under this program, a contract holder can sell to any Government agency with just one source, instead of having separate contracts with each agency.

Key Contract Types under GSA Schedules:

- **Indefinite Delivery Indefinite Quantity (IDIQ)** – provide for an indefinite quantity of services for a fixed time. They are used when GSA cannot determine, above a specified minimum, the precise quantities of supplies or services that the Government will require during the contract period. IDIQs help streamline the contract process and speed service delivery.
- **Blanket Purchase Agreements (BPA)** - an agreement established by a customer with a GSA Schedule contractor to fill repetitive needs for supplies or services (FAR 8.405-3). It simplifies the process for recurring needs, while leveraging a customer's buying power by taking advantage of quantity discounts, saving administrative time, and reducing paperwork.
- **Government-wide Acquisition Contracts (GWACs)** – a type of pre-competed, multiple award (MA) IDIQ contract that allows for the purchase of IT solutions by multiple Federal agencies at once. The scale of the contract results in lower costs than each individual agency could obtain on the open market. Major GWACS include Alliant, OASIS, 8(a) STARS II, and VETS.

3.2 CONTRACTING

Key GSA Contracting Vehicles and Services

CONTRACTING VEHICLES

IT Schedule 70 is a catalog of IT service providers and products that have met certain requirements to be placed in a streamlined acquisition process managed by GSA. IT Schedule 70 (IT70) offerings can be purchased directly on the GSA website. Available products and services range from providing government-wide solutions for desktops and laptops to CDM and cloud cybersecurity services. Using acquisition vehicles like IT Schedule 70 can help agencies shorten procurement cycles by up to 50 percent over the open market, ensure compliance, and obtain the best value.

GSA FEDSIM provides assisted acquisition support for information technology systems and services, and other professional services, to other U.S. Government agencies on a fee for service basis.

Enterprise Infrastructure Solutions (EIS) is a comprehensive solution-based vehicle to address all aspects of Federal agency IT telecommunications, and infrastructure requirements. A successor to Networx, WITS3, and Regional Local Service Agreements, EIS will make it easier for agencies to acquire their enterprise telecommunications and IT infrastructure services from a single source.

Identity Protection Services (IPS) BPA gives Federal agencies access to a variety of identity protection services covering both routine protection services that include consumer credit reports, address verification reports, and credit risk assessments; and recovery services involving suspected or actual breaches of sensitive personally identifiable information.

SERVICES

Highly Adaptive Cybersecurity Services (HACS) are found on IT Schedule 70. These Special Item Numbers (SINs) were developed jointly between DHS and GSA to meet critical capability gaps in agency risk assessments. DHS provided the technical expertise, standard operating procedures, and scope of how these services should be delivered, while GSA validated the qualifications of particular vendors to meet DHS and agency expectations. GSA then added them to IT70 in an easily identifiable manner. These SINs provide agencies quicker access to key, pre-vetted support services, including:

- 132-45A – **Penetration Testing** – security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
- 132-45B – **Incident Response** – help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
- 132-45C – **Cyber Hunt** – responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
- 132-45D – **Risk and Vulnerability Assessment** – services that assess threats and vulnerabilities, assess the level of risk associated with deviations from acceptable configurations, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations.

3.2 CONTRACTING

USAccess offers PIV card issuance to Government agencies through a shared enrollment/activation infrastructure and end-to-end credential maintenance.

Login.gov offers the public secure and private online access to participating Government programs. With one login.gov account, users can sign in to multiple Government agencies.

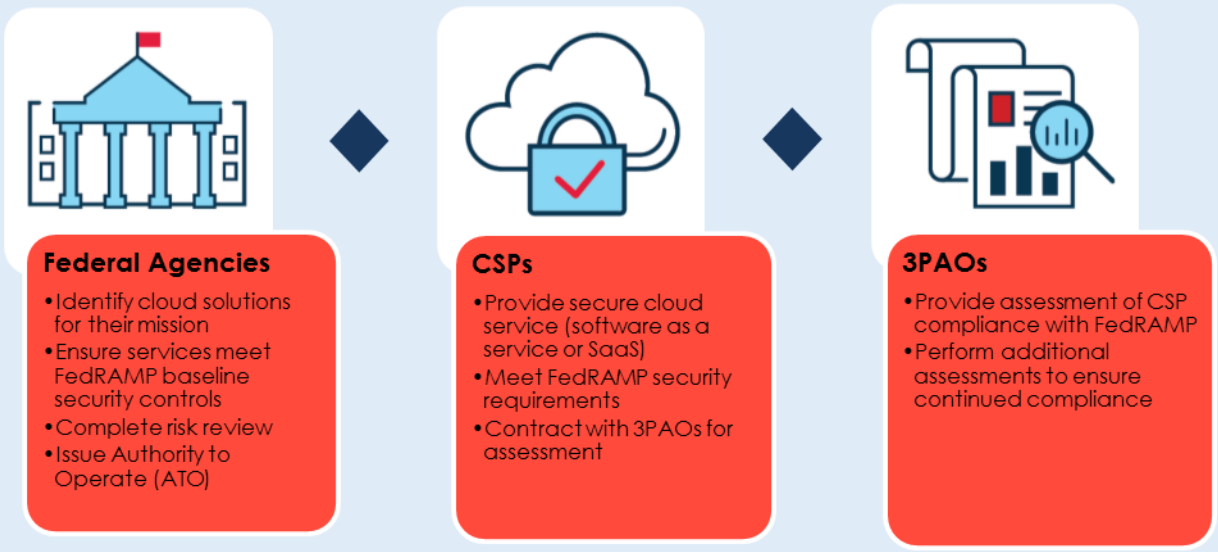
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services (*See* Focus On: FedRAMP below).

3.2 CONTRACTING

Focus On: FedRAMP and Cloud Services

The **FedRAMP Program Management Office (PMO)** provides oversight of FedRAMP processes, developing standards and templates and coordinating with, evaluating, and maintaining the repository of security documentation for Cloud Service Providers (CSPs).

FedRAMP defines three primary players in the process: Federal agencies, CSPs, and Third Party Assessment Organizations (3PAOs).



The **Joint Authorization Board (JAB)** is the primary governance and decision-making body for the FedRAMP program. The JAB reviews and provides joint provisional security authorizations of cloud solutions using a standardized baseline approach. Chief Information Officers from the Department of Defense, the Department of Homeland Security, and the General Services Administration serve on the JAB.

FedRAMP JAB duties and responsibilities:

- Define FedRAMP security authorization requirements
- Approve accreditation criteria for third party assessment organizations
- Establish a priority queue for authorization package reviews
- Review FedRAMP authorization packages
- Grant joint provisional authorizations
- Ensure that provisional authorizations are reviewed and updated regularly

3.3 GOVERNMENT-WIDE SERVICES

Governance, Risk & Compliance

- Cybersecurity Assessment and Risk Management Approach (CARMA)
- High Value Asset (HVA)
- Cybersecurity Coordination, Assessment, and Response (C-CAR)
- Critical Infrastructure Partnership Advisory Council (CIPAC)
- CyberScope & CyberStat Review Program
- Industrial Control Systems Security Assessments

Security Operations

- Advanced Malware Analysis Center (AMAC)
- FireEye / iSight – Threat Intelligence
- .gov Cybersecurity Architecture Review (.govCAR)
- Incident Response – Hunt and Incident Response Team (HIRT)
- EINSTEIN
- Infoblox/Looking Glass – Threat Intelligence

Systems Security

- High Value Asset Assessment
- Risk and Vulnerability Assessment
- Remote Penetration Testing
- Phishing Campaign Assessment
- Industrial Control Systems Security Assessments
- Red Team Assessments
- Threat Hunting

Identity & Access Management

- FIPS 201 Evaluation Program
- PIV/PIV-D Testing
- Physical Access Control System (PACS)
- Server-Based Certificate Validation Protocol (SCVP)

Cloud Security

- Customer Engagement and Solutions Development Division (CESDD)
- Cloud Statement of Objectives (SOO) Templates

APPENDIX

SECTION A

A.1 Example Agency Internal Policies
A.2 Government-wide Policies and Publications
A.3 FISMA Responsibility Breakdowns
A.4 GSA Services
A.5 Glossary

APPENDIX A CONTENTS

A.1 EXAMPLE AGENCY INTERNAL POLICIES

The internal agency policies provided below connect to the NIST Cybersecurity Framework Core Function highlights in Section 2.2. They are purely illustrative and should not be copied wholesale by organizations in place of detailed risk analysis. They are included to give new CISOs a starting point from which to develop policy from scratch, tailored to their organization's needs.

A.1 EXAMPLE AGENCY INTERNAL POLICIES

A.1.1 Secure Asset Management Policy

1. Purpose/Objective

This policy provides requirements for controlling access of hardware, software, and firmware to the network infrastructure.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[1]

B. Federal Information Processing Standards Publication 200, March 2006[2]

C. Office of Management and Budget (OMB) Circular A-130[3]

D. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[4]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security controls as defined in National Institute for Standards and Technology (NIST) 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[5]

A. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

B. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

5. Roles and Responsibilities

Infrastructure Managers must:

A. Maintain an enterprise-wide inventory of components on the network infrastructure.

B. Ensure that all assets connected to the network are authorized and asset ownership is identified.

[1] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
[3] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[5] As applicable to this policy.

Information System Security Officers must:

C. Review and enforce authorization boundary requirements for information systems.

6. Policy

In addition to the roles and responsibilities described above, the following security controls must be met to secure [Agency] information systems. The security controls below are described within the NIST Special Publication 800-53 Rev. 4.[6] [Agency]-specific security requirements are specified within brackets ('[', ']') within the control requirement descriptions. Requirements for information systems will be specified through the control tailoring process and approved through the signature of the security authorization package.

A. Infrastructure Managers must:

NIST #	CONTROL NAME	REQUIREMENT
CM-8 a.	Information System Component Inventory	• Develop and document an inventory of information system components that: • Accurately reflects the current information system; • Includes all components within the authorization boundary of the information system; • Is at the level of granularity deemed necessary for tracking and reporting; and • Includes [where applicable: hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, the component network name and network address]
CM-8 b.	Information System Component Inventory	• Review and update the information system component inventory [monthly]
CM-8 (1)	Information System Component Inventory | Updates During Installations / Removals	• Update the inventory of information system components as an integral part of component installations, removals, and information system updates

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

NIST #	CONTROL NAME	REQUIREMENT
CM-8 (2)	Information System Component Inventory | Automated Maintenance	• Employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components
CM-8 (3) a.	Information System Component Inventory | Automated Unauthorized Component Detection	• Employ automated mechanisms [in near real-time] to detect the presence of unauthorized hardware, software, and firmware components within the information system
CM-8 (3) b.	Information System Component Inventory | Automated Unauthorized Component Detection	• Take the following action when unauthorized components are detected: [disables network access by such devices or quarantine the device from the network until the device is identified, authorized, and is associated with a system and system owner]
CM-8 (4)	Information System Component Inventory | Accountability Information	• Include in the information system component inventory information, a means for identifying by [name; position; role], individuals responsible/accountable for administering those components
CM-8 (7)	Information System Component Inventory | Centralized Repository	• Provide a centralized repository for the inventory of information system components

B. Information System Security Officers must:

NIST #	CONTROL NAME	REQUIREMENT
CM-8 (5)	Information System Component Inventory | No Duplicate Accounting of Components	Verify that all components within the authorization boundary of the information system are not duplicated in other information system inventories

7. Compliance, Enforcement, and Exceptions

A. Compliance: This [Agency] security policy is mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes [Agency] Information Security and Privacy Policy sections X.X.X.

A.1.2 Risk Management Policy

1. Purpose/Objective

This policy provides requirements for periodic assessments of risk on information systems and appropriate response actions in order to effectively manage those risks that have been identified.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[7]

B. Federal Information Processing Standards Publication 200, March 2006[8]

C. Office of Management and Budget (OMB) Circular A-130[9]

D. Office of Management and Budget (OMB) Memorandum M-04-25[10]

E. Office of Management and Budget (OMB) Memorandum M-14-04[11]

F. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[12]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security controls as defined in National Institute for Standards and Technology (NIST) 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[13]

A. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

B. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for satisfying the [Agency] mission and compliance with information security requirements of an information system.

[7] ttps://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[8] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
[9] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[10] https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-25.pdf
[11] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf
[12] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[13] As applicable to this policy.

5. Roles and Responsibilities

Information System Security Officers must:

A. Conduct an assessment of risk on all identified weaknesses in accordance with [Agency] security policies and NIST standards and guidelines.

System Owners must:

B. Provide content for updates to the weaknesses identified in the POA&M. Content to be updated covers all data elements required for POA&M reporting by OMB.

C. Remediate weaknesses on information systems within his / her system portfolio within the maximum tolerable timelines in accordance with [Agency] security policies.

6. Policy

In addition to the roles and responsibilities described above, [Agency] has identified the following as its set of baseline security controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. [Agency]-specific security requirements are specified within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system security plan.

A. The Chief Information Security Officer must:

NIST #	CONTROL NAME	REQUIREMENT
RA-1 a.	Risk Assessment Policy and Procedures	• Develop, document, and disseminate to [Project Managers, Information Security Officers]: • A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls
RA-1 b.	Risk Assessment Policy and Procedures	• Review and update the current: • Risk assessment policy [at least every 3 years]; and • Risk assessment procedures [at least every 2 years]

B. Information System Security Officers must:

NIST #	CONTROL NAME	REQUIREMENT
CA-5 a.	Plan of Action and Milestones	• Develop a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system
CA-5 b.	Plan of Action and Milestones	• Update existing plan of action and milestones [weekly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities
RA-3 a.	Risk Assessment	• Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits
RA-3 b.	Risk Assessment	• Document risk assessment results in [Risk Assessment Report]
RA-3 c.	Risk Assessment	• Review risk assessment results [at least annually]
RA-3 d.	Risk Assessment	• Disseminate risk assessment results to [the System Owner, Authorizing Official, and Chief Information Security Officer in accordance with applicable security procedures]
RA-3 e.	Risk Assessment	• Update the risk assessment [at least annually] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system

7. Compliance, Enforcement, and Exceptions

A. Compliance: This [Agency] security policy is mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this

authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes [Agency] Information Security and Privacy Policy sections X.X.X, X.X.X, and X.X.X.

A.1.3 Access Control Policy

1. Purpose/Objective

This policy provides requirements protecting access to [Agency] information and information systems to support the overall security of its data and mission and requirements related to the authorization of [Agency] users to perform a defined set of actions on a specific set of resources.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[14]

B. Federal Information Processing Standards Publication 200, March 2006[15]

C. Office of Management and Budget (OMB) Circular A-130[16]

D. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[17]

E. National Institute of Standards and Technology (NIST) Special Publication 800-116 Rev. 1, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems, November 2008[18]

F. NIST Special Publication 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security, June 2009[19]

G. NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, June 2014[20]

3. Scope

This policy applies to all [Agency] employees and contractors. This policy sets forth the baseline requirements for security controls as defined in NIST 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[21]

Account Manager: The Account Manager is responsible for granting proper access to [Agency] information systems through information system accounts. This role is often held by system administrators, but it can also be held by members of the business office.

B. Business Program Manager (BPM): The BPM has oversight of the information stored, processed, or transmitted

[14] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[15] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
[16] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[17] ttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf
[19] http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
[20] http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
[21] As applicable to this policy.

by the supporting information system. The BPM represents the program office and the customers during the life of IT projects and coordinates the business needs with the System Owner. The BPM is kept apprised of the progress of the security authorization throughout the process.

C. Facility Manager: The Facility Manager is responsible for establishing security standards and guidelines, implementing physical and environmental security controls, and the monitoring of their implementation at [Agency] facilities. The Facility Manager is also responsible for reviews of facilities' physical access authorizations and of authorizations issued when individuals are reassigned or transferred to other positions within the organization.

D. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for satisfying the [Agency] mission and compliance with information security requirements of an information system.

E. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

F. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

5. Roles and Responsibilities

Account Managers must:

A. Ensure that logical access to [Agency] systems and the network is revoked, or modified, as necessary.

B. Ensure that information system users are uniquely identified. Shared or group accounts are not authorized.

C. Verify that a prospective system user has completed training and provided the required certificate of completion before permitting access [Agency]'s information system.

D. Conduct reviews of accounts requiring access to the information system using defined security procedures.

Managers/Supervisors must:

A. Verify that the new user has completed the required Facilities, Security, and Contracting paperwork to initiate the clearance processes ([Agency] Forms XXXX and XXXX).

B. Process the [Agency] IT Access Request Form ([Agency] Form XXXX) by:

i. Filling in the appropriate sections;

ii. Providing the form to the new user and discussing his or her responsibilities to protect sensitive information;

iii. Verifying the user has completed the [Agency] IT Security Awareness Training;

iv. Receiving a signature for the access request from the user;

v. Signing the form prior to the user gaining access to the system;

vi. Receiving approval signatures from the COR for contractor employees; and

vii. Providing the XXXX form to the Account Manager for access to the system.

C. Notify Facility Managers and Account Managers by 5:00pm of the effective date when [Agency] employees and contractors with access to the system are terminated, transferred, or a need-to-know determination has changed. Employees and contractors on active contracts may regain access to the network by calling and authenticating themselves to the Help Desk. Completion of an additional Form XXXX for network access is not required until 35 days have passed since the last systems access.

D. Support reviews of accounts by reporting changes in access rights for individuals identified during the reviews.

System Owners must:

A. Configure information systems to enforce the most restrictive set of rights and privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

B. Only use approved methods of remote access to information systems.

C. Create access control matrices for information systems within his or her portfolio in accordance with defined security procedures. Access control matrices define roles and permissions for access to the system, conditions for membership in defined roles, and segregation of duties requirements. Segregation of duties requirements are defined in collaboration with the BPM.

D. Receive approval from the CIO or CISO for the use of new methods of remote access prior to implementation based on a risk assessment using NIST SP 800-30, Guide for Conducting Risk Assessments.[22]

Infrastructure Managers must:

A. Develop the [Agency] system use notification message and receive approval from the Office of General Counsel for its use.

B. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.

C. If an employee or contractor changes roles, review their access rights and adjust to fit the new parameters of the role if appropriate.

6. Policy

In addition to the roles and responsibilities described within this policy, [Agency] has identified the following as its set of baseline security controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. Parameters have been defined to meet [Agency] security requirements and are

[22] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

included within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system security plan.

A. Account Manager Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AC-2 d.	Account Management	• Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account
AC-2 e.	Account Management	• Require approvals by [organization managers and/or security representatives] for requests to create information system accounts
AC-2 f.	Account Management	• Create, enable, modify, disable, and remove information system accounts in accordance with [[Agency] access control procedure]
AC-2 g.	Account Management	• Monitor the use of information system accounts
AC-2 j.	Account Management	• Review accounts for compliance with account management requirements [at least monthly following defined security procedures]
AC-2 (11)	Account Management | Usage Conditions	• Configure the information system to enforce [requirements to meet [Agency] mission and business objectives] for [use of guest / anonymous and temporary accounts]
AC-2 (12) a.	Account Management | Account Monitoring / Atypical Usage	• Monitor information system accounts for [atypical usage depending on the account and role]

NIST #	CONTROL NAME	REQUIREMENT
AC-2 (12) b.	Account Management | Account Monitoring / Atypical Usage	• Report atypical usage of information system accounts to [the Information System Security Officer]
AC-2 (13)	Account Management | Disable Accounts for High-Risk Individuals	• Disable accounts of users posing a significant risk within [24 hours] of discovery of the risk
AC-6 (5)	Least Privilege | Privileged Accounts	• Restrict privileged accounts on the information system to [roles defined in the system access control matrix]

B. Chief Information Security Officer Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AC-1 a.	Access Control Policy and Procedures	• Develop, document, and disseminate to [Project Managers, Information System Security Officers]: • An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Procedures to facilitate the implementation of the access control policy and associated access controls
AC-1 b.	Access Control Policy and Procedures	• Review and update the current: • Access control policy [at least every 3 years]; and • Access control procedures [at least every 2 years]

C. Business Program Manager Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AC-2 i.	Account Management	• Authorize access to the information system based on: • A valid access authorization; • Intended system usage; and • Other attributes as required by the Program Office or associated missions/business functions
AC-2 (5)	Account Management | Inactivity Logout	• Require that users log out when [at the completion of the work day].
AC-5 a.	Separation of Duties	• Separate [duties of individuals as necessary to prevent conflict of interest activity without collusion]
AC-6	Least Privilege	• Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions
AC-6 (1)	Least Privilege | Authorize Access to Security Functions	• Explicitly authorize access to [security functions including but not limited to establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, modifying device configurations, etc.)]
AC-6 (2)	Least Privilege | Non-Privileged Access for Non-Security Functions	• Require that users of information system accounts, or roles, with access to [security functions including but not limited to establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, modifying device configurations, etc.)], use non-privileged accounts or roles, when accessing non-security functions
AC-6 (3)	Least Privilege | Network Access to Privileged Commands	• Authorize network access to [privileged commands for managing accounts, applications, systems, or security information] only for [compelling operational needs after consultation with the ISSO] and documents the rationale for such access in the security plan for the information system

A.1 EXAMPLE AGENCY INTERNAL POLICIES

NIST #	CONTROL NAME	REQUIREMENT
AC-14 a.	Permitted Actions without Identification or Authentication	• Identify [actions, in consultation with the CISO,] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions
AC-20 a.	Use of External Information Systems	• Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: • Access the information system from external information systems;
AC-20 b.	Use of External Information Systems	• Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: • Process, store, or transmit organization-controlled information using external information systems.
AC-20 (1)	Use of External Information Systems	• Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the Program Office: • Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or • Retains approved information system connection or processing agreements with the organizational entity hosting the external information system
AC-22 a.	Publicly Accessible Content	• Designate individuals authorized to post information onto a publicly accessible information system
AC-22 b.	Publicly Accessible Content	• Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information
AC-22 c.	Publicly Accessible Content	• Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included
AC-22 d.	Publicly Accessible Content	• Review the content on the publicly accessible information system for nonpublic information [at least annually] and removes such information, if discovered

D. Manager / Supervisor Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AC-2 h.	Account Management	• Notify account managers: • When accounts are no longer required; • When users are terminated or transferred; and • When individual information system usage or need-to-know changes

E. System Owner Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AC-2 a.	Account Management	• Identify and select the following types of information system accounts to support organizational missions/business functions: [account types defined within the system access control matrix]
AC-2 b.	Account Management	• Assign account managers for information system accounts
AC-2 c.	Account Management	• Establish conditions for group and role membership
AC-2 (1)	Account Management | Automated System Account Management	• Employ automated mechanisms to support the management of information system accounts
AC-2 (2)	Account Management | Removal of Temporary / Emergency Accounts	• Configure the information system to automatically [disable] temporary and emergency accounts after [no more than 7 calendar days]

A.1 EXAMPLE AGENCY INTERNAL POLICIES

NIST #	CONTROL NAME	REQUIREMENT
AC-2 (3)	Account Management | Disable Inactive Accounts	• Configure the information system to automatically disable inactive accounts after [14 calendar days of inactivity]
AC-2 (4)	Account Management | Automated Audit Actions	• Configure the information system to automatically audit account creation, modification, enabling, disabling, and removal actions, and notify [Account Managers]
AC-3	Access Enforcement	• Configure the information system to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies
AC-4	Information Flow Enforcement	• Configure the information system to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on [[Agency] Access Control, Boundary Protection, and Information Sharing policies]
AC-5 b.	Separation of Duties	• Document separation of duties of individuals
AC-5 c.	Separation of Duties	• Define information system access authorizations to support separation of duties
AC-6 (9)	Least Privilege | Auditing Use of Privileged Accounts	• Configure the information system to audit the execution of privileged functions
AC-6 (10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	• Configure the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/ countermeasures
AC-7 a.	Unsuccessful Logon Attempts	• Configure the information system to: • Enforce a limit of [three] consecutive invalid logon attempts by a user during a [indefinite time period];

A.1 EXAMPLE AGENCY INTERNAL POLICIES

NIST #	CONTROL NAME	REQUIREMENT
AC-7 b.	Unsuccessful Logon Attempts	• Configure the information system to: • Automatically [lock the account until unlocked by an administrator] when the maximum number of unsuccessful attempts is exceeded
AC-8 a.	System Use Notification	• Configure the information system to display to users [an [Agency] approved Warning Banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: • Users are accessing a U.S. Government information system; • Information system usage may be monitored, recorded, and subject to audit; • Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and • Use of the information system indicates consent to monitoring and recording;
AC-8 b.	System Use Notification	• Configure the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system
AC-8 c.	System Use Notification	• Configure the publicly-available information system to: • Display system use information [at initial entry], before granting further access; • Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and • Include a description of the authorized uses of the system
AC-10	Concurrent Session Control	• Configure the information system to limits the number of concurrent sessions for each [system account] to [one]
AC-11 a.	Session Lock	• Configure the information system to prevent further access to the system by initiating a session lock after [15 minutes] of inactivity or upon receiving a request from a user

A.1 EXAMPLE AGENCY INTERNAL POLICIES

NIST #	CONTROL NAME	REQUIREMENT
AC-11 b.	Session Lock	• Configure the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures
AC-11 (1)	Session Lock	• Configure the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image
AC-12	Session Termination	• Configure the information system to automatically terminate a user session after [30 minutes of inactivity or loss of connection]
AC-14 b.	Permitted Actions without Identification or Authentication	• Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication
AC-17 a.	Remote Access	• Establish and document usage restrictions, configuration/ connection requirements, and implementation guidance for each type of remote access allowed
AC-17 b.	Remote Access	• Authorize remote access to the information system prior to allowing such connections
AC-17 (1)	Remote Access	• Configure the information system to monitor and control remote access methods
AC-17 (2)	Remote Access	• Configure the information system to implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions
AC-17 (3)	Remote Access	• Configure the information system to route all remote accesses through [, in compliance with Trusted Internet Connection requirements, a limited number of] managed network access control points
AC-17 (4) a.	Remote Access	• Authorize the execution of privileged commands and access to security-relevant information via remote access only for [compelling operational needs after consultation with the ISSO]
AC-17 (4) b.	Remote Access	• Document the rationale for such access in the security plan for the information system

NIST #	CONTROL NAME	REQUIREMENT
AC-18 a.	Wireless Access	• Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access
AC-18 b.	Wireless Access	• Authorize wireless access to the information system prior to allowing such connections
AC-18 (1)	Wireless Access	• Configure the information system to protect wireless access to the system using authentication of [users, devices, or both as necessary,] and encryption
AC-18 (4)	Wireless Access	• Identify and explicitly authorize users allowed to independently configure wireless networking capabilities
AC-18 (5)	Wireless Access	• Select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries
AC-19 a.	Access Control for Mobile Devices	• Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices
AC-19 b.	Access Control for Mobile Devices	• Authorize the connection of mobile devices to organizational information systems
AC-19 (5)	Access Control for Mobile Devices	• Employ [full-device encryption] to protect the confidentiality and integrity of information on [mobile computers / devices that carry sensitive agency data]
AC-20 (2)	Use of External Information Systems	• [Restrict] the use of organization-controlled portable storage devices by authorized individuals on external information systems
AC-20 (3)	Use of External Information Systems	• [Prohibit] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information
AC-21 a.	Information Sharing	• Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [circumstances where user discretion is required for sharing sensitive information]

NIST #	CONTROL NAME	REQUIREMENT
AC-21 b.	Information Sharing	• Employ [automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions

7. Compliance, Enforcement, and Exceptions

A. Compliance: The requirements imposed by this [Agency] security policy are mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the CISO, an [Agency] supervisor, manager, associate director, or office director, as appropriate. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes section X.X and all subsections of the Information Security and Privacy Policy and section X of the Information Security and Privacy Policy Addendum.

A.1.4 System Maintenance Policy

1. Purpose/Objective

This policy provides requirements for the performance of maintenance on information systems by authorized personnel in a secure manner.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[23]

B. Federal Information Processing Standards Publication 200, March 2006[24]

C. Office of Management and Budget Circular A-130[25]

D. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[26]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security controls as defined in National Institute for Standards and Technology (NIST) 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[27]

A. Account Manager: The Account Manager is responsible for granting proper access to [Agency] information systems through information system accounts. This role is often held by system administrators, but it can also be held by members of the business office.

B. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

C. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

[23] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[24] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[25] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

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

[27] As applicable to this policy.

D. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for satisfying the [Agency] mission and compliance with information security requirements of an information system.

5. Roles and Responsibilities

Account Managers must:

A. Disable authenticators for maintenance accounts until required to perform maintenance.

System Owners must:

A. Complete routine preventative and regular maintenance activities without adversely affecting system security or operations.

B. Follow configuration management and change control processes for maintenance activities.

C. Specify information system components that, when not operational, result in increased risk to the organization, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include: firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

D. Restrict maintenance activities to a list of authorized maintenance organizations or personnel.

E. Obtain approval from the Infrastructure Manager prior to removing system components from [Agency] facilities for off-site maintenance or repairs.

6. Policy

In addition to the roles and responsibilities described above, [Agency] has identified the following as its set of baseline security controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. [Agency]-specific security requirements are specified within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system security plan.

A. The Chief Information Security Officer must:

NIST #	CONTROL NAME	REQUIREMENT
MA-1 a.	System Maintenance Policy and Procedures	• Develop, document, and disseminate to [Project Managers, Information Security Officers]: • A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls

NIST #	CONTROL NAME	REQUIREMENT
MA-1 b.	System Maintenance Policy and Procedures	• Review and update the current: • System maintenance policy [at least every 3 years]; and • System maintenance procedures [at least every 2 years]
MA-2 c.	Controlled Maintenance	• Require that [the Infrastructure Manager] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs

B. Information System Security Officers must:

NIST #	CONTROL NAME	REQUIREMENT
MA-2 e.	Controlled Maintenance	• Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions
MA-4 (2)	Nonlocal Maintenance | Document Nonlocal Maintenance	• Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

C. System Owners must:

NIST #	CONTROL NAME	REQUIREMENT
MA-2 a.	Controlled Maintenance	• Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
MA-2 b.	Controlled Maintenance	• Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
MA-2 d.	Controlled Maintenance	• Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

NIST #	CONTROL NAME	REQUIREMENT
MA-2 e.	Controlled Maintenance	• Include [date and time of maintenance; name of the individual performing the maintenance; name of escort, if necessary; description of the maintenance performed; and, for Moderate and High systems, the list of equipment removed or replaced (including identification numbers, if applicable)] in organizational maintenance records.
MA-2 (2) a.	Controlled Maintenance | Automated Maintenance Activities	• Employ automated mechanisms to schedule, conduct, and document maintenance and repairs.
MA-2 (2) b.	Controlled Maintenance | Automated Maintenance Activities	• Produce up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.
MA-3	Maintenance Tools	• Approve, control, and monitor information system maintenance tools.
MA-3 (1)	Maintenance Tools | Inspect Tools	• Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized
MA-3 (2)	Maintenance Tools | Inspect Media	• Check media containing diagnostic and test programs for malicious code before the media are used in the information system.
MA-3 (3)	Maintenance Tools | Prevent Unauthorized Removal	• Prevent the unauthorized removal of maintenance equipment containing organizational information by: • Verifying that there is no organizational information contained on the equipment; • Sanitizing or destroying the equipment; • Retaining the equipment within the facility; or • Obtaining an exemption from [the Chief Information Security Officer] explicitly authorizing removal of the equipment from the facility
MA-4 a.	Nonlocal Maintenance	• Approve and monitor nonlocal maintenance and diagnostic activities.

NIST #	CONTROL NAME	REQUIREMENT
MA-4 b.	Nonlocal Maintenance	• Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.
MA-4 c.	Nonlocal Maintenance	• Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
MA-4 d.	Nonlocal Maintenance	• Maintain records for nonlocal maintenance and diagnostic activities.
MA-4 e.	Nonlocal Maintenance	• Terminate session and network connections when nonlocal maintenance is completed.
MA-4 (3)	Nonlocal Maintenance | Comparable Security / Sanitization	• Require that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or • Remove the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitize the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspect and sanitize the component (with regard to potentially malicious software) before reconnecting the
MA-5 a.	Maintenance Personnel	• Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
MA-5 b.	Maintenance Personnel	• Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.
MA-5 c.	Maintenance Personnel	• Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

NIST #	CONTROL NAME	REQUIREMENT
MA-5 (1) a.	Maintenance Personnel | Individuals without Appropriate Access	• Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: • Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; • Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured
MA-5 (1) b.	Maintenance Personnel | Individuals without Appropriate Access	• Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.
MA-6	Timely Maintenance	• Obtain maintenance support and/or spare parts for [critical information system components and/or key information technology components defined by SOs] within [72 hours] of failure.

7. Compliance, Enforcement, and Exceptions

A. Compliance: This [Agency] security policy is mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information

systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes the Information Security and Privacy Policy Handbook section X.X.

A.1.5 Continuous Monitoring Policy

1. Purpose/Objective

This policy identifies the requirements for maintaining ongoing awareness of information security and privacy vulnerabilities and threats to support organizational risk management decisions.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[28]

B. Federal Information Processing Standards Publication 200, March 2006[29]

C. Office of Management and Budget Circular A-130[30]

D. National Institute of Standards and Technology, Special Publication 800-53, Revision 4[31]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security and privacy controls as defined in NIST 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the control baseline for information systems to more closely align security and privacy requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[32]

A. Chief Information Security Officer (CISO): The CISO carries out the responsibilities of the Chief Information Officer (CIO) under the Federal Information Security Modernization Act of 2014 (FISMA).

B. Chief Privacy Officer (CPO): The CPO is responsible for ensuring compliance with applicable privacy requirements and managing privacy risks. The CPO reviews privacy risks throughout the lifecycle of information.

C. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

[28] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[29] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[30] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

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

[32] As applicable to this policy.

D. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

E. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for satisfying the [Agency] mission and compliance with information security and privacy requirements of an information system.

F. Security Control Assessor (SCA): An individual, group, or organization responsible for conducting comprehensive assessments of the security controls employed within an information system to determine their overall effectiveness.

G. Security Operations Center (SOC): The SOC is responsible for the development, implementation, and maintenance of [Agency]'s Incident Response Plan. The SOC is the primary component of [Agency]'s incident response capabilities, including monitoring, handling, and response, and supports the SO with technical security support.

5. Roles and Responsibilities

The Chief Information Security Officer (CISO) must:

A. Define roles and responsibilities for carrying out the security activities documented within the continuous monitoring strategy.

The Chief Privacy Officer (CPO) must:

B. Define roles and responsibilities for carrying out the privacy activities documented within the continuous monitoring strategy.

Information System Security Officers must:

C. Conduct ongoing security status monitoring of the system inventory and plan of action and milestones metrics for each system within his or her portfolio in accordance with the continuous monitoring strategy.

D. Use Federal and [Agency] standards to evaluate risks and provide recommendations to manage risks identified through the continuous monitoring program.

Infrastructure Managers must:

E. Conduct ongoing security status monitoring of hardware asset management and software asset management metrics in accordance with the continuous monitoring strategy.

System Owners must:

F. Implement response actions to address results of the analysis of security-related and privacy-related information identified by the continuous monitoring program for each system within his or her portfolio.

G. Review and update privacy documentation in accordance with the frequencies defined in the continuous monitoring strategy.

Security Control Assessors must:

H. Conduct ongoing assessments of security and privacy controls in accordance with the continuous monitoring strategy.

The Security Operations Center must:

I. Conduct ongoing security status monitoring of configuration settings management and vulnerability management metrics in accordance with the continuous monitoring strategy.

6. Policy

In addition to the roles and responsibilities described within this policy, [Agency] has identified the following as its set of baseline security and privacy controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. Parameters have been defined to meet [Agency] security and privacy requirements and are included within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system security plan. The selection of privacy controls is subject to the CPO's, or CPO's designee's, signature of the system security plan.

A. Chief Information Security Officer Requirements:

NIST #	CONTROL NAME	REQUIREMENT
CA-7 a.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Establishment of [agency-level and system-level information security metrics for each security capability] to be monitored
CA-7 b.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Establishment of [frequencies for each information security metric] for monitoring and [risk-based, cost-effective frequencies] for assessments supporting such monitoring
CA-7 c.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Ongoing security control assessments in accordance with the organizational continuous monitoring strategy

NIST #	CONTROL NAME	REQUIREMENT
CA-7 d.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy
CA-7 e.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Correlation and analysis of security-related information generated by assessments and monitoring
CA-7 f.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Response actions to address results of the analysis of security-related information
CA-7 g.	Continuous Monitoring	• Develop a continuous monitoring strategy and implements a continuous monitoring program that includes: • Reporting the security status of organization and the information system to [the CIO for the organization and Authorizing Official for the system] [at least quarterly]
CA-7 (1)	Continuous Monitoring | Independent Assessment	• Employ assessors or assessment teams with [a level of independence defined within the continuous monitoring strategy] to monitor the security controls in the information system on an ongoing basis

B. Security Control Assessor Requirements:

NIST #	CONTROL NAME	REQUIREMENT
AR-4	Privacy Monitoring and Auditing	• Monitor and audit privacy controls and internal privacy policy [in accordance with the continuous monitoring strategy] to ensure effective implementation.

7. Compliance, Enforcement, and Exceptions

A. Compliance: The requirements imposed by this [Agency] security policy are mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for enforcement and compliance of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the CISO, an [Agency] supervisor, manager, associate director or office director, as appropriate. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs. The CISO will direct any requests for exceptions to the privacy provisions within the policy to the CPO.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes section X.X.X of the Information Security and Privacy Policy.

A.1.6 Malicious Code Policy

1. Purpose/Objective

This policy provides requirements for protections against viruses, worms, Trojan horses, spyware, and other forms of malicious code.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[33]

B. Federal Information Processing Standards (FIPS) Publication 200, March 2006[34]

C. Office of Management and Budget (OMB) Circular A-130[35]

D. National Institute for Standards and Technology (NIST), Special Publication 800-53, Revision 4[36]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security controls as defined in NIST 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[37]

A. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

B. Security Operations Center (SOC): The SOC is responsible for the development, implementation, and maintenance of [Agency]'s Incident Response Plan. The SOC is the primary component of [Agency]'s incident response capabilities, including monitoring, handling, and response, and supports the System Owner with technical security support.

5. Roles and Responsibilities

Infrastructure Managers must:

A. Deploy malicious code protection mechanisms at entry and exit points into the network infrastructure, including:

[33] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[34] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[35] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

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

[37] As applicable to this policy.

remote access servers, proxy servers, web servers, workstations, and mobile devices.

The Security Operations Center must:

B. Scan hardware assets for malware prior to authorizing a remote access connection to the network.

C. Block outbound connections from the network to known phishing websites and IP addresses.

6. Policy

In addition to the roles and responsibilities described above, [Agency] has identified the following as its set of baseline security controls consistent with the minimum security requirements defined in the NIST FIPS 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. [Agency]-specific security requirements are specified within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the Chief Information Security Officer's (CISO), or CISO's designee's, signature of the system security plan.

A. Infrastructure Managers must:

NIST #	CONTROL NAME	REQUIREMENT
SI-3 a.	Malicious Code Protection	• Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code
SI-8 a.	Spam Protection	• Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages
SI-16	Memory Protection	• Configure the information system to implement [data execution prevention and address space layout randomization] to protect its memory from unauthorized code execution

B. The Security Operations Center must:

NIST #	CONTROL NAME	REQUIREMENT
SI-3 b.	Malicious Code Protection	• Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures

NIST #	CONTROL NAME	REQUIREMENT
SI-3 c. 1.	Malicious Code Protection	• Configure malicious code protection mechanisms to: • Perform periodic scans of the information system [at least weekly] and real-time scans of files from external sources at [endpoints for web traffic and network entry / exit points for e-mail traffic] as the files are downloaded, opened, or executed in accordance with organizational security policy;
SI-3 c. 2.	Malicious Code Protection	• Configure malicious code protection mechanisms to: • [block malicious code or quarantine malicious code and send an alert to an administrator] in response to malicious code detection
SI-3 d.	Malicious Code Protection	• Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
SI-3 (2)	Malicious Code Protection | Automatic Updates	• Configure the information system to automatically update malicious code protection mechanisms
SI-8 b.	Spam Protection	• Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures
SI-8 (1)	Spam Protection | Central Management	• Centrally manage spam protection mechanisms
SI-8 (2)	Spam Protection | Automatic Updates	• Configure the information system to automatically update spam protection mechanisms

7. Compliance, Enforcement, and Exceptions

A. Compliance: The requirements imposed by this [Agency] security policy are mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes the following sections of the Information Security and Privacy Policy:

- X.X.X Malicious Code Protection (SI-3); and
- X.X.X Spam Protection (SI-8).

A.1.7 Incident Response Policy

1. Purpose/Objective

This policy provides requirements for establishing an operational incident handling capability for [Agency] information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[38]

B. Federal Information Processing Standards Publication 200, March 2006[39]

C. Office of Management and Budget (OMB) Circular A-130[40]

D. Office of Management and Budget (OMB) Memorandum M-17-12[41]

E. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[42]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security and privacy controls as defined in NIST 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the control baseline for information systems to more closely align security and privacy requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[43]

A. Business Program Manager (BPM): The BPM has oversight of the information stored, processed, or transmitted by the supporting information system. The BPM represents the program office and the customers during the life of IT projects and coordinates the business needs with the System Owner. The BPM is kept apprised of the progress of the security authorization throughout the process.

B. Chief Information Security Officer (CISO): The CISO carries out the responsibilities of the Chief Information Officer (CIO) under the Federal Information Security Modernization Act of 2014 (FISMA).

C. Chief Privacy Officer (CPO): The CPO is responsible for ensuring compliance with applicable privacy requirements and managing privacy risks. The CPO reviews privacy risks throughout the lifecycle of information.

[38] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[39] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[40] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[41] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

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

[43] As applicable to this policy.

D. Incident: The act of violating an explicit or implied security policy.[44]

E. Information System Security Officer (ISSO): An individual with the detailed knowledge and expertise required to manage the security aspects of an information system. The ISSO is the principal advisor for the System Owner to obtain guidance in security matters and support the dissemination of security requirements. The ISSO role is held by information security specialists in [Agency] Cybersecurity and provides independent review and oversight of security processes involving the design, development, and implementation of information systems.

F. Security Operations Center (SOC): The SOC is responsible for the development, implementation, and maintenance of [Agency]'s Incident Response Plan. The SOC is the primary component of [Agency]'s incident response capabilities, including monitoring, handling, and response, and supports the SO with technical security support.

G. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for satisfying the [Agency] mission and compliance with information security requirements of an information system.

5. Roles and Responsibilities

All [Agency] information system users must:

A. Report all suspected incidents to the SOC [CONTACT REMOVED].

Business Program Managers must:

B. Notify business partners with established data sharing agreements of impacts to information systems as a result of incident response activities, such as access to information systems being revoked or information systems being taken off line.

The Security Operations Center must:

C. Initiate a ticket and notify appropriate parties upon receipt of a suspected incident.

D. Report incidents internally and to United States Computer Emergency Readiness Team (US-CERT), in accordance with the US-CERT Federal Incident Notification Guidelines and the [Agency] Cyber Protection and Defense Manual. Program Offices must not send incident reports directly to US-CERT.

6. Policy

In addition to the roles and responsibilities described above, [Agency] has identified the following as its set of baseline security and privacy controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. [Agency]-specific security and privacy requirements are specified within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system

[44] https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition

security plan. The selection of privacy controls is subject to the CPO's, or CPO's designee's, signature of the system security plan.

A. The Chief Information Security Officer must:

NIST #	CONTROL NAME	REQUIREMENT
IR-1 a.	Incident Response Policy and Procedures	• Develop, document, and disseminate to [Project Managers, Information System Security Officers]: • An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Procedures to facilitate the implementation of the incident response policy and associated incident response controls
IR-1 b.	Incident Response Policy and Procedures	• Review and update the current: • Incident response policy [at least every 3 years]; and • Incident response procedures [at least every 2 years]
IR-6 a.	Incident Reporting	• Require personnel to report suspected security incidents to the organizational incident response capability within [immediately (no more than 30 minutes after becoming aware of the incident)]

B. The Chief Privacy Officer must:

NIST #	CONTROL NAME	REQUIREMENT
SE-2 a.	Privacy Incident Response	• Develop and implement a Privacy Incident Response Plan
SE-2 b.	Privacy Incident Response	• Provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan

C. The Security Operations Center must:

NIST #	CONTROL NAME	REQUIREMENT
IR-3	Incident Response Testing	• Test the incident response capability for the information system [at least annually] using [scenario based exercises] to determine the incident response effectiveness and documents the results
IR-3 (2)	Incident Response Testing | Coordination with Related Plans	• Coordinate incident response testing with organizational elements responsible for related plans
IR-4 a.	Incident Handling	• Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
IR-4 b.	Incident Handling	• Coordinate incident handling activities with contingency planning activities
IR-4 c.	Incident Handling	• Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly
IR-4 (1)	Incident Handling | Automated Incident Handling Processes	• Employ automated mechanisms to support the incident handling process
IR-4 (4)	Incident Handling | Information Correlation	• Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response
IR-5	Incident Monitoring	• Track and document information system security incidents

NIST #	CONTROL NAME	REQUIREMENT
IR-5 (1)	Incident Monitoring | Automated Tracking / Data Collection / Analysis	• Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information
IR-6 b.	Incident Reporting	• Report security incident information to [[Agency] personnel, interagency partners, and the public per the [Agency] Cyber Protection and Defense Manual]
IR-6 (1)	Incident Reporting | Automated Reporting	• Employ automated mechanisms to assist in the reporting of security incidents
IR-7	Incident Response Assistance	• Provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents
IR-7 (1)	Incident Response Assistance | Automation Support for Availability of Information / Support	• Employ automated mechanisms to increase the availability of incident response-related information and support

NIST #	CONTROL NAME	REQUIREMENT
IR-8 a.	Incident Response Plan	• Develop an incident response plan that: • Provides the organization with a roadmap for implementing its incident response capability; • Describes the structure and organization of the incident response capability; • Provides a high-level approach for how the incident response capability fits into the overall organization; • Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; • Defines reportable incidents; • Provides metrics for measuring the incident response capability within the organization; • Defines the resources and management support needed to effectively maintain and mature an incident response capability; and • Is reviewed and approved by [CISO]
IR-8 b.	Incident Response Plan	• Distribute copies of the incident response plan to [the CIO, SOs, ISSOs, and additional staff as necessary]
IR-8 c.	Incident Response Plan	• Review the incident response plan [Quarterly]
IR-8 d.	Incident Response Plan	• Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing [at least Quarterly]
IR-8 e.	Incident Response Plan	• Communicate incident response plan changes to [the CIO, CISO, SOs, ISSOs, and other impacted staff quarterly]
IR-8 f.	Incident Response Plan	• Protect the incident response plan from unauthorized disclosure and modification

7. Compliance, Enforcement, and Exceptions

A. Compliance: The requirements imposed by this [Agency] security policy are mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs. The CISO will direct any requests for exceptions to the privacy provisions within the policy to the CPO.

8. Contact Information

Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes sections X.X, X.X.X, and X.X.X through X.X.X of the Information Security and Privacy Policy.

A.1.8 Contingency Planning Policy

1. Purpose/Objective

This policy provides requirements for the recovery of mission and business services after a disruption to the information system.

2. Authorities

The authorities for this policy include:

A. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014[45]

B. Federal Information Processing Standards Publication 200, March 2006[46]

C. Office of Management and Budget (OMB) Circular A-130[47]

D. National Institute for Standards and Technology, Special Publication 800-53, Revision 4[48]

E. National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, May 2010, Contingency Planning Guide for Federal Information Systems[49]

3. Scope

This policy applies to all [Agency] employees and contractors. This [Agency] policy sets forth the baseline requirements for security controls as defined in NIST 800-53 and assigns programmatic responsibility to specific offices and positions. As described below, tailoring of the security control baseline for information systems to more closely align security requirements with [Agency]'s mission and business requirements and environments of operation may be appropriate.

4. Definitions[50]

A. Chief Information Security Officer (CISO): The CISO carries out the responsibilities of the Chief Information Officer (CIO) under the Federal Information Security Modernization Act of 2014 (FISMA).

B. Infrastructure Manager (IM): Manages the network or datacenter that handles [Agency] applications or data, at all locations where it is maintained, and is responsible for providing in-depth information security support for [Agency]'s infrastructure.

C. System Owner (SO): The program manager responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The SO is responsible for

[45] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[46] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[47] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

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

[49] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[50] As applicable to this policy.

satisfying the [Agency] mission and compliance with information security requirements of an information system.

5. Roles and Responsibilities

Infrastructure Managers must:

A. Conduct an annual full-functional disaster recovery (DR) test on the infrastructure environment.

B. Coordinate DR testing of the infrastructure with SOs responsible for managing systems that reside on the infrastructure environment.

System Owners must:

A. Conduct a Business Impact Analysis (BIA) for the information system, in coordination with the business sponsor, to identify essential missions and business functions and associated contingency requirements.

B. Conduct full-scale, functional Contingency Plan (CP) testing in coordination with the infrastructure DR testing for systems with high-impact availability requirements as defined by the security categorization and BIA processes. Include reference(s) to the coordinated effort in the CP test results.

C. Conduct functional CP testing, at a minimum, for systems with moderate-impact availability requirements as defined by the security categorization and BIA processes.

D. Conduct table-top CP testing, at a minimum, for systems with low-impact availability requirements as defined by the security categorization and BIA processes.

E. Provide CP test results to the CISO annually for evidence and reporting.

6. Policy

In addition to the roles and responsibilities described above, [Agency] has identified the following as its set of baseline security controls consistent with the minimum security requirements defined in the NIST Federal Information Processing Standards (FIPS) 200 and the high impact security control baseline defined in Special Publication (SP) 800-53 Rev. 4. [Agency]-specific security requirements are specified within brackets ('[. . .]') within the control requirement descriptions. This baseline set of security controls is subject to the control tailoring process in accordance with [Agency] security authorization procedures, consistent with FIPS 200 and SP 800-53 Rev. 4, and approved through the CISO's, or CISO's designee's, signature of the system security plan.

A.1 EXAMPLE AGENCY INTERNAL POLICIES

A. The Chief Information Security Officer must:

NIST #	CONTROL NAME	REQUIREMENT
CP-1 a.	Contingency Planning Policy and Procedures	• Develop, document, and disseminate to [Project Managers, Information Security Officers]: • A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls
CP-1 b.	Contingency Planning Policy and Procedures	• Review and update the current: • Contingency planning policy [at least every 3 years]; and • Contingency planning procedures [at least every 2 years]

B. Infrastructure Managers must:

NIST #	CONTROL NAME	REQUIREMENT
CP-8	Telecommunications Services	• Establish alternate telecommunications services including necessary agreements to permit the resumption of [information system operations] for essential missions and business functions within [at least 12 hours for High systems (The time frame for resumption of essential missions and business functions for Moderate systems must be based on the Recovery Time Objective (RTO))] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites
CP-8 (1) a.	Telecommunications Services | Priority of Service Provisions	• Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives)
CP-8 (1) b.	Telecommunications Services | Priority of Service Provisions	• Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier

NIST #	CONTROL NAME	REQUIREMENT
CP-8 (2)	Telecommunications Services | Single Points of Failure	• Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services
CP-8 (3)	Telecommunications Services | Separation of Primary / Alternate Providers	• Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats
CP-8 (4) a.	Telecommunications Services | Provider Contingency Plan	• Require primary and alternate telecommunications service providers to have contingency plans
CP-8 (4) b.	Telecommunications Services | Provider Contingency Plan	• Review provider contingency plans to ensure that the plans meet organizational contingency requirements
CP-8 (4) c.	Telecommunications Services | Provider Contingency Plan	• Obtain evidence of contingency testing/training by providers [annually]

C. System Owners must:

NIST #	CONTROL NAME	REQUIREMENT
CP-2 a.	Contingency Plan	• Develop a contingency plan for the information system that: • Identifies essential missions and business functions and associated contingency requirements; • Provides recovery objectives, restoration priorities, and metrics; • Addresses contingency roles, responsibilities, assigned individuals with contact information; • Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; • Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and • Is reviewed and approved by [System Owners]
CP-2 b.	Contingency Plan	• Distribute copies of the contingency plan to [key contingency personnel and other related organizational elements or entities]
CP-2 c.	Contingency Plan	• Coordinate contingency planning activities with incident handling activities
CP-2 d.	Contingency Plan	• Review the contingency plan for the information system [at least annually]
CP-2 e.	Contingency Plan	• Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
CP-2 f.	Contingency Plan	• Communicate contingency plan changes to [key contingency personnel and other related organizational elements or entities]
CP-2 g.	Contingency Plan	• Protect the contingency plan from unauthorized disclosure and modification
CP-2 (1)	Contingency Plan | Coordinate with Related Plans	• Coordinate contingency plan development with organizational elements responsible for related plans

NIST #	CONTROL NAME	REQUIREMENT
CP-2 (2)	Contingency Plan | Capacity Planning	• Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations
CP-2 (3)	Contingency Plan | Resume Essential Missions / Business Functions	• Plan for the resumption of essential missions and business functions within [at least 12 hours for High systems (The time frame for resumption of essential missions and business functions for Moderate systems must be based on the Recovery Time Objective (RTO))] of contingency plan activation
CP-2 (4)	Contingency Plan | Resume All Missions / Business Functions	• Plan for the resumption of all missions and business functions within [the Recovery Time Objective (RTO) established within the Business Impact Analysis (BIA)] of contingency plan activation
CP-2 (5)	Contingency Plan | Continue Essential Missions / Business Functions	• Plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites
CP-2 (8)	Contingency Plan | Identify Critical Assets	• Identify critical information system assets supporting essential missions and business functions
CP-4 a.	Contingency Plan Testing	• Test the contingency plan for the information system [at least annually] using [[Agency] defined and information system specific tests and exercises such as checklist, walk-through/tabletop, simulation, parallel, full interrupt] to determine the effectiveness of the plan and the organizational readiness to execute the plan
CP-4 b.	Contingency Plan Testing	• Reviews the contingency plan test results
CP-4 c.	Contingency Plan Testing	• Initiates corrective actions, if needed

NIST #	CONTROL NAME	REQUIREMENT
CP-4 (1)	Contingency Plan Testing | Coordinate with Related Plans	• Coordinate contingency plan testing with organizational elements responsible for related plans
CP-4 (2) a.	Contingency Plan Testing | Alternate Processing Site	• Test the contingency plan at the alternate processing site:
CP-4 (2) b.	Contingency Plan Testing | Alternate Processing Site	• To familiarize contingency personnel with the facility and available resources;
CP-6 a.	Alternate Storage Site	• Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information
CP-6 b.	Alternate Storage Site	• Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site
CP-6 (1)	Alternate Storage Site | Separation from Primary Site	• Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats
CP-6 (2)	Alternate Storage Site | Recovery Time / Point Objectives	• Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives
CP-6 (3)	Alternate Storage Site | Accessibility	• Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions

NIST #	CONTROL NAME	REQUIREMENT
CP-7 a.	Alternate Processing Site	• Establish an alternate processing site including necessary agreements to permit the transfer and resumption of [information system operations] for essential missions/business functions within [at least 12 hours for High systems (The time frame for resumption of essential missions and business functions for Moderate systems must be based on the Recovery Time Objective (RTO))] when the
CP-7 b.	Alternate Processing Site	• Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption
CP-7 c.	Alternate Processing Site	• Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site
CP-7 (1)	Alternate Processing Site | Separation from Primary Site	• Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats
CP-7 (2)	Alternate Processing Site | Accessibility	• Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions
CP-7 (3)	Alternate Processing Site | Priority of Service	• Develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives)
CP-7 (4)	Alternate Processing Site | Preparation for Use	• Prepare the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions
CP-9 a.	Information System Backup	• Conduct backups of user-level information contained in the information system [periodically (Low), weekly (Moderate), and daily (High) for file shares on the network; end users are responsible for backup and recovery functions for desktops, notebooks, and hand-held computers]

NIST #	CONTROL NAME	REQUIREMENT
CP-9 b.	Information System Backup	• Conduct backups of system-level information contained in the information system [periodically (Low), weekly (Moderate), and daily (High)]
CP-9 c.	Information System Backup	• Conduct backups of information system documentation including security-related documentation [periodically (Low), weekly (Moderate), and daily (High) for file shares on the network; end users are responsible for backup and recovery functions for desktops, notebooks, and hand-held computers]
CP-9 d.	Information System Backup	• Protect the confidentiality, integrity, and availability of backup information at storage locations
CP-9 (1)	Information System Backup | Testing for Reliability / Integrity	• Test backup information [at least annually (A frequency of quarterly is recommended for High systems and semi-annually is recommended for Moderate systems)] to verify media reliability and information integrity
CP-9 (2)	Information System Backup | Test Restoration Using Samples	• Use a sample of backup information in the restoration of selected information system functions as part of contingency plan testing
CP-9 (3)	Information System Backup | Separate Storage for Critical Information	• Store backup copies of [the operating system and other critical information system software, as well as, copies of the information system inventory (including hardware, software, and firmware components)] in a separate facility or in a fire-rated container that is not collocated with the operational system
CP-9 (5)	Information System Backup | Transfer to Alternate Storage Site	• Transfer information system backup information to the alternate storage site [at a transfer rate consistent with established recovery time objectives (RTO) and recovery point objectives (RPO)]
CP-10	Information System Recovery and Reconstitution	• Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure

NIST #	CONTROL NAME	REQUIREMENT
CP-10 (2)	Information System Recovery and Reconstitution | Transaction Recovery	• Assure the information system implements transaction recovery for systems that are transaction-based
CP-10 (4)	Information System Recovery and Reconstitution | Restore Within Time Period	• Provide the capability to restore information system components within [established recovery time objectives (RTO)] from configuration-controlled and integrity-protected information representing a known, operational state for the components

7. Compliance, Enforcement, and Exceptions

A. Compliance: The requirements imposed by this [Agency] security policy are mandatory for all employees and contractors. This policy uses the plain language guidelines for conveying requirements. The following convention is used:

- "must" for an obligation;
- "must not" for a prohibition;
- "may" for a discretionary action; and
- "should" for a recommendation.

B. Enforcement: The CISO is responsible for compliance and enforcement of this policy and, consistent with this authority, may take action necessary to prevent risk to [Agency] information or information systems. Violations, or suspected violations, should be reported to the Cybersecurity Program; see Section 8 for contact information. Violations of the policy may result in the loss or limitation of access to [Agency] information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and potential referral for appropriate criminal/civil proceedings.

C. Exceptions: Policy waivers are approved deviations from a policy requirement that are subject to approval of the CISO. The CISO maintains the formal request form, which must be submitted by Associate Directors or Office Heads to the CISO for review and approval. Each waiver must be submitted with a compelling business case justification and risk assessment conducted by an ISSO. Waivers will be reviewed on a case-by-case basis. Waivers granted for an information system will remain valid until the Authorization to Operate for the system expires. Waivers granted for an office will remain valid until the next review and update of this policy occurs.

8. Contact Information

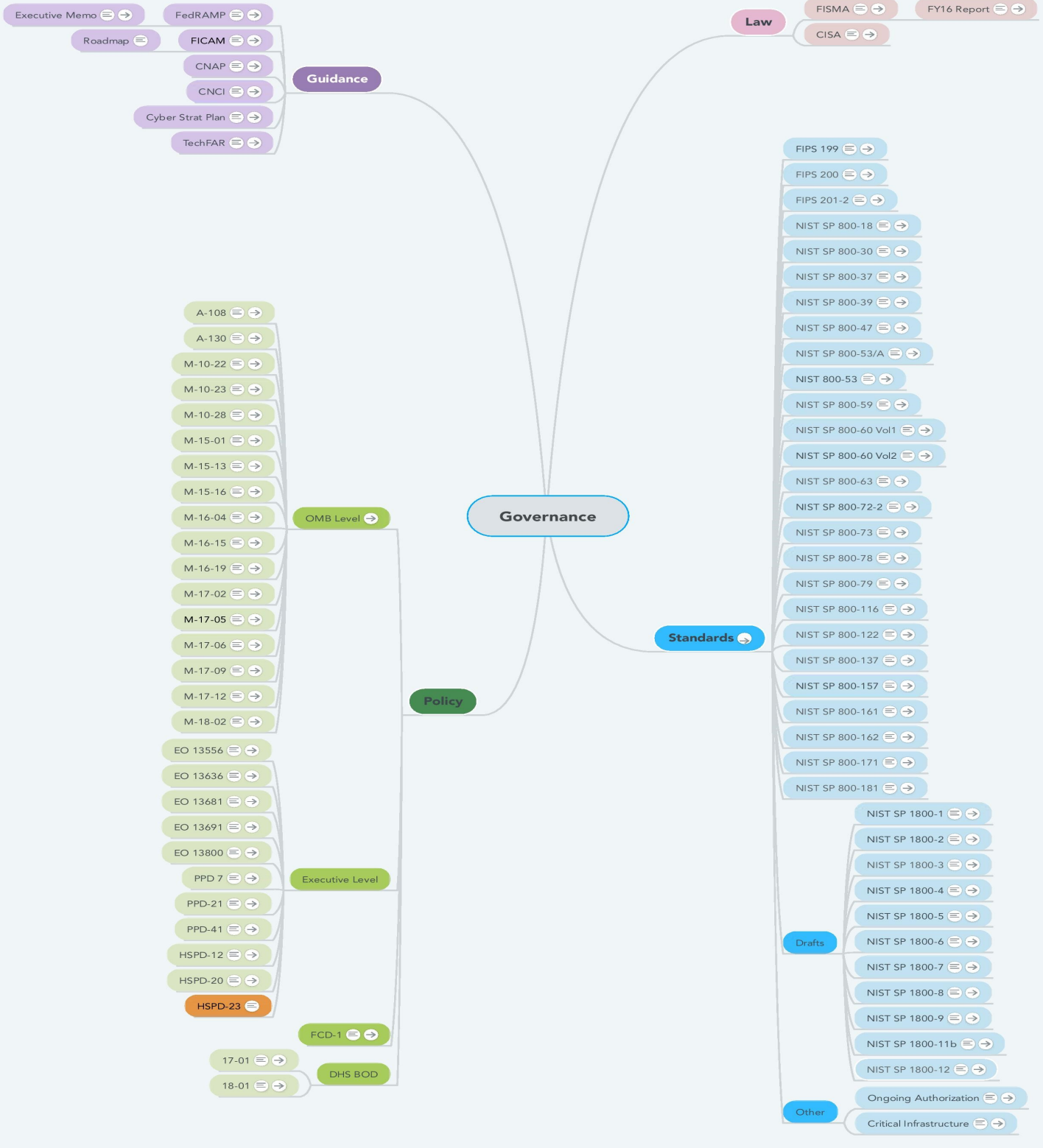
Any questions or concerns regarding this policy should be directed to:

[AGENCY CONTACT INFORMATION]

9. Expiration and Renewal

This policy is in effect as of the date on this memorandum and should be reviewed and renewed every three years. This policy supersedes sections X.X, X.X.X, X.X.X, and X.X.X through X.X.X of the Information Security and Privacy Policy.

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS



A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

The table below gathers all of the government-wide policies and publications that impact the CISO's role. The policies are presented in chronological order with the most recent first. Some issue dates are approximate.

Policy or Publication	Code or short	Issue Date
Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements	M-18-02	10/16/17
Binding Operational Directive 18-01: Enhance Email and Web Security	BOD 18-01	10/16/17
Derived Personal Identity Verification (PIV) Credentials	NIST SP 1800-12	9/29/17
Attribute Based Access Control (2nd Draft)	NIST SP 1800-3	9/20/17
Binding Operational Directive 17-01: Removal of Kaspersky-Branded Products	BOD 17-01	9/13/17
Data Integrity: Recovering from Ransomware and Other Destructive Events	NIST SP 1800-11	9/6/17
Access Rights Management for the Financial Services Sector	NIST SP 1800-9	8/31/17
NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	NIST SP 800-53	8/1/17
National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	NIST SP 800-181	8/1/17
NIST Special Publication 800-63, Electronic Authentication Guideline.	NIST SP 800-63	6/1/17
Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	M-17-25	5/19/17
Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	EO 13800	5/11/17

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
Securing Wireless Infusion Pumps in Healthcare Delivery Organizations	NIST SP 1800-8	5/8/17
US-CERT Federal Incident Notification Guidelines		4/1/17
FY 2016 FISMA14: Annual Report to Congress		3/10/17
Situational Awareness for Electric Utilities	NIST SP 1800-7	2/16/17
Federal Continuity Directive 1 - Federal Executive Branch National Continuity Program and Requirements, February 2008.	FCD-1	1/7/17
Preparing for and Responding to a Breach of Personally Identifiable Information	M-17-12	1/3/17
Circular No. A-108: Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act	A-108	12/23/16
Management of Federal High Value Assets	M-17-09	12/9/16
NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.	NIST SP 800-171	12/1/16
Policies for Federal Agency Public Websites and Digital Services	M-17-06	11/8/16
Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements	M-17-05	11/4/16
Domain Name Systems-Based Electronic Mail Security	NIST SP 1800-6	11/2/16
Data Center Optimization Initiative (DCOI)	M-16-19	8/1/16

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
Circular No. A-130: Managing Information as a Strategic Resource	A-130	7/27/16
Federal Government Coordination Architecture for Significant Cyber Incidents	PPD-41	7/26/16
Preparation, Submission, and Execution of the Budget	Circular A-11	7/1/16
Federal Cybersecurity Workforce Strategy	M-16-15	6/12/16
Gift Basket on Mitigating Insider Threats		4/1/16
Cybersecurity National Action Plan	CNAP	2/9/16
Federal Cybersecurity Research and Development Strategic Plan		2/4/16
Mobile Device Security: Cloud and Hybrid Builds	NIST SP 1800-4	11/2/15
Cybersecurity Strategy Implementation Plan (CSIP)	M-16-04	10/30/15
Cybersecurity Act of 2015 (including CISA)		10/27/15
IT Asset Management: Financial Services	NIST SP 1800-5	10/26/15
Identity and Access Management for Electric Utilities	NIST SP 1800-2	8/25/15
Securing Electronic Health Records on Mobile Devices	NIST SP 1800-1	7/28/15

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
Multi-Agency Science and Technology Priorities for the FY 2017 Budget	M-15-16	7/9/15
NIST Special Publication 800-79, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).	NIST SP 800-79	7/1/15
FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity		6/12/15
Policy to Require Secure Connections across Federal Websites and Web Services	M-15-13	6/8/15
NIST Special Publication 800-73, Interfaces for Personal Identity Verification.	NIST SP 800-73	5/1/15
NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.	NIST SP 800-78	5/1/15
NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.	NIST SP 800-161	4/1/15
Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing	EO 13691	2/20/15
NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans	NIST SP 800-53A	12/18/14
Federal Information Security Modernization Act of 2014	FISMA 14	12/18/14
NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification Credentials.	NIST SP 800-157	12/1/14
Executive Order 13681 Improving the Security of Consumer Financial Transactions	EO 13681	10/17/14
Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices	M-15-01	10/3/14

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
TechFAR		8/8/14
NIST Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management.		6/1/14
NIST Framework for Improving Critical Infrastructure Cybersecurity.		4/16/18
NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.	NIST SP 800-162	1/1/14
Enhancing the Security of Federal Information and Information Systems	M-14-03	11/8/13
NIST Federal Information Processing Standards Publication 201, Personal Identity Verification of Federal Employees and Contractors	FIPS PUB 201-2	8/1/13
NIST Special Publication 800-76-2, Biometric Specifications for Personal Identity Verification.	NIST SP 800-76-2	7/1/13
Presidential Policy Directive -- Critical Infrastructure Security and Resilience	PPD-21	2/12/13
Executive Order 13636 Improving Critical Infrastructure Cybersecurity	EO 13636	2/12/13
NIST Special Publication 800-30, Guide for Conducting Risk Assessments	NIST SP 800-30	9/1/12
Computer Security Incident Handling Guide	NIST SP 800-61	8/1/12
Security Authorization of Information Systems in Cloud Computing Environments		12/8/11
Security Authorization of Information Systems in Cloud Computing Environments	(FedRAMP memo)	12/8/11

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
Federal Identity, Credential and Access Management Roadmap and Implementation Guidance		12/2/11
Trustworthy Cyberspace: Strategic Plan for Cybersecurity R&D Programs		12/1/11
NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.	NIST SP 800-137	9/1/11
NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View	NIST SP 800-39	3/1/11
Executive Order 13556 Controlled Unclassified Information	EO 13556	11/4/10
Clarifying Cybersecurity Responsibilities and Activities of EOP and DHS	M-10-28	7/6/10
Guidance for Online Use of Web Measurement and Customization Technologies	M-10-22	6/25/10
Guidance for Agency Use of Third-Party Websites and Applications	M-10-23	6/25/10
NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems	NIST SP 800-34	5/1/10
NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).	NIST SP 800-122	4/1/10
NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	NIST SP 800-37	2/1/10
Cyberspace Policy Review		5/29/09
Comprehensive National Cybersecurity Initiative	CNCI	5/1/09
NIST Special Publication 800-116, Guidelines for the Use of PIV Credentials in Physical Access Control Systems (PACS).	NIST SP 800-116	11/1/08

A.2 GOVERNMENT-WIDE POLICIES AND PUBLICATIONS

Policy or Publication	Code or short	Issue Date
Securing the Federal Government's Domain Name System Infrastructure	M-08-23	8/22/08
NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.	NIST SP 800-60	8/1/08
HSPD - 23 Cybersecurity Policy	HSPD - 23	1/8/08
Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection	HSPD-7	12/3/07
Homeland Security Presidential Directive 20 (National Security Presidential Directive 51) - National Continuity Policy	HSPD-20	5/9/07
NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems	FIPS PUB 200	3/1/06
NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems	NIST SP 800-18	2/1/06
Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors	HSPD-12	8/27/04
Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors	HSPD-12	8/27/04
NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems	FIPS PUB 199	2/1/04
NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.	NIST SP 800-59	8/1/03
E-Government Act of 2002	FISMA 2002	12/17/02
NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems	NIST SP 800-47	8/1/02

A.3 FISMA RESPONSIBILITY BREAKDOWNS

The tables in this Appendix break the language in FISMA down by which party is responsible for each action. For convenience, we have only included the responsibilities assigned to Federal agencies, DHS, and OMB in this document. Please see the full FISMA law for the complete roles and responsibilities it assigns.

A.3.1 FISMA Responsibility Breakdown for Agencies

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	b(1)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	b(2)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— policies and procedures that— (A) are based on the risk assessments required by paragraph (1); (B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with— (i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;
§ 3554. Federal agency responsibilities	b(3)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	b(4)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— (A) information security risks associated with their activities; and (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;
§ 3554. Federal agency responsibilities	b(5)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing— (A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); (B) may include testing relied on in an evaluation under section 3555; and (C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	b(6)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
§ 3554. Federal agency responsibilities	b(7)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— procedures for detecting, reporting, and responding to security incidents, which— (A) shall be consistent with the standards and guidelines described in section 3556(b); (B) may include using automated tools; and (C) shall include— (i) mitigating risks associated with such incidents before substantial damage is done; (ii) notifying and consulting with the Federal information security incident center established in section 3556; and (iii) notifying and consulting with, as appropriate— (I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel; (II) an office designated by the President for any incident involving a national security system; (III) for a major incident, the committees of Congress described in subsection (c)(1)—(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and (bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and (IV) any other agency or office, in accordance with law or as directed by the President; and

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	b(8)	Agencies	AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	c(1)	Agencies	AGENCY REPORTING.— ANNUAL REPORT.— (A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including— (i) a description of each major information security incident or related sets of incidents, including summaries of— (I) the threats and threat actors, vulnerabilities, and impacts relating to the incident; (II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred; (III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and (IV) the detection, response, and remediation actions; (ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems; (iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including— (I) the number of individuals whose information was affected by the major information security incident; and (II) a description of the information that was breached or exposed; and (iv) any other information as the Director or the Secretary, in consultation with the Director, may require. (B) UNCLASSIFIED REPORT.— (i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex. (ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	c(2)	Agencies	AGENCY REPORTING.— OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.
§ 3554. Federal agency responsibilities	d(1)	Agencies	PERFORMANCE PLAN.— In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of— (A) the time periods; and (B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).
§ 3554. Federal agency responsibilities	d(2)	Agencies	PERFORMANCE PLAN.— The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).
§ 3554. Federal agency responsibilities	e	Agencies	PUBLIC NOTICE AND COMMENT.— Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.
§ 3556. Federal information security incident center	b	Agencies (operating or exercising control of a national security system)	NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3557. National security systems		Agencies (operating or exercising control of a national security system)	The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
§ 3557. National security systems		Agencies (operating or exercising control of a national security system)	The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
§ 3557. National security systems		Agencies (operating or exercising control of a national security system)	The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—complies with the requirements of this subchapter.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	a(1)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall be responsible for— (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of— (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; (B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including— (i) information security standards promulgated under section 11331 of title 40; (ii) operational directives developed by the Secretary under section 3553 (b); (iii) policies and procedures issued by the Director; and (iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and (C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	a(2)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through— (A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems; (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements; (C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and (D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	a(3)	Agencies (the head of each agency)	[LEGISLATIVE DEFINITION OF CISO ROLE] IN GENERAL.—The head of each agency shall delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including— (A) designating a senior agency information security officer who shall— (i) carry out the Chief Information Officer's responsibilities under this section; (ii) possess professional qualifications, including training and experience, required to administer the functions described under this section; (iii) have information security duties as that official's primary duty; and (iv) head an office with the mission and resources to assist in ensuring agency compliance with this section; (B) developing and maintaining an agencywide information security program as required by subsection (b); (C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40; (D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and (E) assisting senior agency officials concerning their responsibilities under paragraph (2);

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3554. Federal agency responsibilities	a(4)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;
§ 3554. Federal agency responsibilities	a(5)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;
§ 3554. Federal agency responsibilities	a(6)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and
§ 3554. Federal agency responsibilities	a(7)	Agencies (the head of each agency)	IN GENERAL.—The head of each agency shall ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).
§ 3555. Annual independent evaluation	e(1)	Agencies (the head of each agency)	AGENCY REPORTING.— Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.
§ 3555. Annual independent evaluation	a(1)	Agencies (Inspector General or independent external auditor)	IN GENERAL.— Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3555. Annual independent evaluation	a(2)	Agencies (Inspector General or independent external auditor)	IN GENERAL.— Each evaluation under this section shall include— (A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; (B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and (C) separate presentations, as appropriate, regarding information security relating to national security systems.
§ 3555. Annual independent evaluation	d	Agencies (Inspector General or independent external auditor)	EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.
§ 3555. Annual independent evaluation	e(2)	Agencies (Inspector General or independent external auditor)	AGENCY REPORTING.— To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.
§ 3555. Annual independent evaluation	f	Agencies (Inspector General or independent external auditor)	PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.
§ 3555. Annual independent evaluation	b(1)	Agencies (Inspector General or independent external auditor)	INDEPENDENT AUDITOR.—Subject to subsection (c)— for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3555. Annual independent evaluation	b(2)	Agencies (Inspector General or independent external auditor)	INDEPENDENT AUDITOR.—Subject to subsection (c)— for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.
§ 3555. Annual independent evaluation	c(1)	Agencies (an entity designated by the agency head)	NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed— only by an entity designated by the agency head; and
§ 3555. Annual independent evaluation	c(2)	Agencies (an entity designated by the agency head)	NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed— in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

A.3.2 FISMA Responsibility Breakdown for DHS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	b(1)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);
§ 3553. Authority and functions of the Director and the Secretary	b(2)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including— (A) requirements for reporting security incidents to the Federal information security incident center established under section 3556; (B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1); (C) requirements for the mitigation of exigent risks to information systems; and (D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	b(3)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including monitoring agency implementation of information security policies and practices;
§ 3553. Authority and functions of the Director and the Secretary	b(4)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;
§ 3553. Authority and functions of the Director and the Secretary	b(5)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	b(6)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by— (A) operating the Federal information security incident center established under section 3556; (B) upon request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement; (C) compiling and analyzing data on agency information security; and (D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems; and
§ 3553. Authority and functions of the Director and the Secretary	b(7)	DHS (Secretary of)	SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.
§ 3553. Authority and functions of the Director and the Secretary	d	DHS (Secretary of)	NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	f(1)	DHS (Secretary of)	CONSIDERATION.—IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.
§ 3553. Authority and functions of the Director and the Secretary	f(2)	DHS (Secretary of)	CONSIDERATION.—DIRECTIVES.—The Secretary shall— (A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and (B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.
§ 3553. Authority and functions of the Director and the Secretary	f(3)	DHS (Secretary of)	CONSIDERATION.—RULE OF CONSTRUCTION.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.
§ 3553. Authority and functions of the Director and the Secretary	g	DHS (Secretary of)	EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.
§ 3556. Federal information security incident center	a(1)	DHS (Secretary of)	IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to— provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3556. Federal information security incident center	a(2)	DHS (Secretary of)	IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to— compile and analyze information about incidents that threaten information security;
§ 3556. Federal information security incident center	a(3)	DHS (Secretary of)	IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to— inform operators of agency information systems about current and potential information security threats, and vulnerabilities;
§ 3556. Federal information security incident center	a(4)	DHS (Secretary of)	IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to— provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and
§ 3556. Federal information security incident center	a(5)	DHS (Secretary of)	IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to— consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.
§ 3558. Effect on existing law	c	DHS (Secretary of)	CONTINUOUS DIAGNOSTICS.—During the 2 year period beginning on the date of enactment of this Act, the Director of the Office of Management and Budget, with the assistance of the Secretary of Homeland Security, shall include in each report submitted under section 3553(c) of title 44, United States Code, as added by subsection (a), an assessment of the adoption by agencies of continuous diagnostics technologies, including through the Continuous Diagnostics and Mitigation program, and other advanced security tools to provide information security, including challenges to the adoption of such technologies or security tools.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3558. Effect on existing law	d(2)	DHS (Secretary of)	BREACHES.— NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.
§ 3558. Effect on existing law	d(3)	DHS (Secretary of)	BREACHES.— REPORTS.— (A) DIRECTOR OF OMB.—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis— (i) assess agency implementation of data breach notification policies and guidelines in aggregate; and (ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code. (B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.
§ 3553. Authority and functions of the Director and the Secretary	c(1)	DHS (Secretary of) (in consultation with OMB Director)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	c(2)	DHS (Secretary of) (in consultation with OMB Director)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a description of the threshold for reporting major information security incidents;
§ 3553. Authority and functions of the Director and the Secretary	c(3)	DHS (Secretary of) (in consultation with OMB Director)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a summary of the results of evaluations required to be performed under section 3555;
§ 3553. Authority and functions of the Director and the Secretary	c(4)	DHS (Secretary of) (in consultation with OMB Director)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—an assessment of agency compliance with standards promulgated under section 11331 of title 40; and
§ 3553. Authority and functions of the Director and the Secretary	c(5)	DHS (Secretary of) (in consultation with OMB Director)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

A.3.3. FISMA Responsibility Breakdown for OMB

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	a(1)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;
§ 3553. Authority and functions of the Director and the Secretary	a(2)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of— (A) information collected or maintained by or on behalf of an agency; or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
§ 3553. Authority and functions of the Director and the Secretary	a(3)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including ensuring that the Secretary carries out the authorities and functions under subsection (b);
§ 3553. Authority and functions of the Director and the Secretary	a(4)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including coordinating the development of standards and guidelines 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;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	a(5)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and
§ 3553. Authority and functions of the Director and the Secretary	a(6)	OMB (Director of)	DIRECTOR.—The Director shall oversee agency information security policies and practices, including coordinating information security policies and procedures with related information resources management policies and procedures.
§ 3553. Authority and functions of the Director and the Secretary	d	OMB (Director of)	NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.
§ 3553. Authority and functions of the Director and the Secretary	g	OMB (Director of)	EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.
§ 3558. Effect on existing law	b(1)	OMB (Director of)	MAJOR INCIDENT.—The Director of the Office of Management and Budget shall— develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and
§ 3558. Effect on existing law	b(2)	OMB (Director of)	MAJOR INCIDENT.—The Director of the Office of Management and Budget shall— provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3558. Effect on existing law	c	OMB (Director of)	CONTINUOUS DIAGNOSTICS.—During the 2 year period beginning on the date of enactment of this Act, the Director of the Office of Management and Budget, with the assistance of the Secretary of Homeland Security, shall include in each report submitted under section 3553(c) of title 44, United States Code, as added by subsection (a), an assessment of the adoption by agencies of continuous diagnostics technologies, including through the Continuous Diagnostics and Mitigation program, and other advanced security tools to provide information security, including challenges to the adoption of such technologies or security tools.
§ 3558. Effect on existing law	d(1)	OMB (Director of)	BREACHES.— REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require— (A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall— (i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and (ii) include— (I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred; (II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals; (III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and (IV) an estimate of whether and when the agency will provide notice to affected individuals; and (B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3558. Effect on existing law	d(3)	OMB (Director of)	BREACHES.— REPORTS.— (A) DIRECTOR OF OMB.—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis— (i) assess agency implementation of data breach notification policies and guidelines in aggregate; and (ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code. (B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.
§ 3553. Authority and functions of the Director and the Secretary	c(1)	OMB (Director of) (in consultation with Secretary of Homeland Security)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);
§ 3553. Authority and functions of the Director and the Secretary	c(2)	OMB (Director of) (in consultation with Secretary of Homeland Security)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a description of the threshold for reporting major information security incidents;
§ 3553. Authority and functions of the Director and the Secretary	c(3)	OMB (Director of) (in consultation with Secretary of Homeland Security)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—a summary of the results of evaluations required to be performed under section 3555;

A.3 FISMA RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
§ 3553. Authority and functions of the Director and the Secretary	c(4)	OMB (Director of) (in consultation with Secretary of Homeland Security)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—an assessment of agency compliance with standards promulgated under section 11331 of title 40; and
§ 3553. Authority and functions of the Director and the Secretary	c(5)	OMB (Director of) (in consultation with Secretary of Homeland Security)	REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

A.4 GSA SERVICES CATALOG

The table below was provided by GSA to demonstrate the government-wide services and acquisition vehicles available to agencies. A short description is provided for each service. Please follow the links to the services for details and ordering information.

Service	Short Description	Category
FedSIM	GSA FEDSIM provides assisted acquisition support for information technology systems and services, and professional services, to other U.S. Government agencies on a fee for service basis.	Cyber Acquisition
BPAs	BPAs offer an excellent option for federal agencies and Schedule contractors alike, providing convenience, efficiency, and reduced costs.	Cyber Acquisition
Networx	A broad range of domestic and international network services including managed security services through the Managed Trusted Internet Protocol Services (MTIPS) program	Cyber Acquisition
IT Schedule 70	IT Schedule 70 delivers federal, state, and local customer agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions.	Cyber Acquisition
FedRAMP	GSA-led assessment and authorization program that is mandatory for cloud infrastructures offered to the federal government.	Cyber Acquisition
Cloud.gov	GSA provides a secure infrastructure platform as a service to federal teams (i.e., offers a cloud-hosting product line)	Cyber Acquisition

A.4 GSA SERVICES CATALOG

Service	Short Description	Category
Login.gov	Federated credential management for public-private programs	Cyber Acquisition
FASt Lane	Assisting established IT vendors with being listed on IT Sched 70	Cyber Acquisition
Springboard	Assisting innovative IT vendors w/ fewer than 2 years' experience with being listed on IT Sched 70	Cyber Acquisition
Project Boise	Examining ways to shorten the timeline associated with getting a system authorized to operate on federal networks.	Cyber Engagement
ICAM	Security disciplines that enable the right individual to access the right resource, at the right time, for the right reason.	Cyber Policy
DCOI	GSA OGP is the data center shared services coordinator, serving as a trusted agent and SME to assist data center providers and consumers by providing guidance on technology advancements, innovation, cybersecurity, and best practices	Cyber Policy
CIO Council	The Office of Executive Councils provides dedicated support to Federal interagency management councils, increasing their effectiveness in solving challenges across agencies, spurring innovation and improving policy outcomes.	Cyber Policy
PACS	GSA provides guidance and support to federal agencies to standardize the implementation of Physical/Cyber security systems across government	Cyber Policy

A.4 GSA SERVICES CATALOG

Service	Short Description	Category
SSA	GSA and the Federal Protective Service (at DHS) are co-leads with the role to coordinate information sharing, resilience, and protective measures for Government Facilities, the critical information they contain, and the strategic locations they inhabit, where the risk of intrusion may be heightened.	Cyber Policy
TFS	Ongoing GSA program to collaborate with industry to certify solutions for US government agencies to use in online identity proofing and authentication services	Cyber Policy
DCIM	GSA provides standards and best practices regarding the best tools and processes to catalogue, manage and monitor data center assets	Cyber Policy
Federalist	Secure website publishing service	Cyber Services
FPKI	Operation and maintenance of FPKI cybersecurity critical infrastructure, foundational to Federal Identity, Credential, and Access Management (FICAM) to secure information technology assets government-wide.	Cyber Services
USAccess	Offers PIV card issuance to government agencies through a shared enrollment/activation infrastructure and end-to-end credential maintenance	Cyber Services
Dotgov	The Gov Domain is the Top Level Internet Domain for the United States Government and many state, local and tribal governments.	Cyber Services
HACS	HACS Special Item Numbers (SINs) provide agencies quicker access to key, pre-vetted cybersecurity support services	Cyber Services

A.4 GSA SERVICES CATALOG

Service	Short Description	Category
CDM	CDM SINs provide agencies quicker access to key, pre-vetted cybersecurity tools	Cyber Services
Bug Bounty	Program offering a monetary reward (or "bounty") to qualified people who identify issues (or "bugs") with program-identified services.	Cyber Services
GSA Smartpay	GSA rollout of secure microchip & PIN enabled charge cards to its account holders (purchase, travel, integrated, and some fleet card users)	Cyber Services

A.5 GLOSSARY

The following definitions apply for the purposes of this document. All definitions are based on those in OMB Circular A-130 – Managing Information as a Strategic Resource unless otherwise cited.

Agency	any executive agency or department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. NOTE: The term "agency" is used to refer to both large and small agencies for the purposes of this handbook. The term "organization" is also used to refer to large agencies, small agencies, and components within agencies that may have a CISO or equivalent position.
Breach	as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII, or (2) an authorized user accesses PII for an unauthorized purpose.[51]
Binding Operational Directive (BOD)	a compulsory direction from the Department of Homeland Security to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in
Chief Information Officer (CIO)	the senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.

[51] M-18-02 – Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf

A.5 GLOSSARY

Chief Information Security Officer (CISO)	the senior information security officer to whom the Chief Information Officer delegates tasks related to information security under FISMA (35 U.S.C. § 3554)
Critical infrastructure	systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters (42 U.S.C. § 5195c(e)).
Cybersecurity	prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. NOTE: In this handbook, cybersecurity and information security are used interchangeably, but this is not the case in all Federal publications and policies.
Incident	an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (44 U.S.C. § 3552).
Information System	means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.
Information	any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
Information Security	means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; b) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and c) Availability, which means ensuring timely and reliable access to and use of information (44 U.S.C. § 3552). NOTE: In this handbook, cybersecurity and information security are used interchangeably, but this is not the case in all Federal publications and policies.

A.5 GLOSSARY

Information security continuous monitoring (ISCM)	maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions. NOTE: The terms continuous and ongoing in this context mean that security controls and agency risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect agency information.
Information technology (IT)	any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use (40 U.S.C. § 11101).
Major incident	any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, the economy of the United States; or to the public confidence, civil liberties, or public health and safety of the American people.[52]
Personally identifiable information (PII)	information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Privacy impact assessment (PIA)	an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

[52] M-18-02 – Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf

A.5 GLOSSARY

Risk	a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risk can include both information security and privacy risks.
Risk management	the program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
Risk management strategy	the description of how an agency intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.
Security category	the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.
Security control	the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security control assessment	the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security control baseline	the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Senior Agency Official for Privacy (SAOP)	the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.
Tailoring	the process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls.


CIO
COUNCIL


CHIEF INFORMATION SECURITY OFFICER COUNCIL