CHAPTER 8

Federal Government Information Security and Privacy Regulations

IN A 2009 SPEECH, then U.S. President Barack Obama said that America's digital infrastructure is a "strategic national asset."[1] He urged a broad plan to protect the security and privacy of federal information systems, stating that the nation's digital infrastructure must be better protected. Both the federal government and private organizations have a role to play.

This chapter reviews how the federal government protects its information systems. These systems hold personal data about U.S. residents, conduct the business of running the country, hold sensitive security data, and are used for the nation's defense. This chapter reviews the security and privacy laws that protect these systems.

Chapter 8 Topics

This chapter covers the following topics and concepts:

- What the information security challenges facing the federal government are
- What the Federal Information Security Management Act (FISMA) does
- How the federal government protects privacy in information systems
- What import and export control laws are
- What some case studies and examples are

Chapter 8 Goals

When you complete this chapter, you will be able to:

- Describe the federal government's information security challenges
- Explain the main requirements under the Federal Information Security Management Act
- Describe the role of the National Institute of Standards and Technology (NIST) in creating information security standards
- Discuss approaches to protecting national security systems (NSSs)

- Describe how the U.S. federal government protects privacy in information systems
- Review import and export control laws

Information Security Challenges Facing the Federal Government

In 2010, Vivek Kundra, then federal chief information officer (CIO), said that the government's computers are attacked millions of times each day.[2] In 2018, federal agencies reported over 31,000 information security incidents involving federal information technology (IT) systems.[3] That government IT systems are frequently attacked and suffer information security incidents is not surprising. Government computer systems hold data that is critical for government operations. They hold data on people living in the United States, including employment, tax, and citizenship data. They also hold data on businesses operating in the United States, as well as data that are used to protect the United States from threats.

NOTE

You can view analytics for U.S. government websites at https://analytics.usa.gov/. At 7:00 a.m. ET on May 16, 2020, there were over 140,000 people on government webpages. The most popular websites were for the U.S. Postal Service and Internal Revenue Service.

The government faces many of the same information security challenges that private entities face. Federal IT systems and the data in them are attractive targets for criminals:

- Hackers stole the background investigation records from the Office of Personnel Management (OPM). The sensitive personnel files on over 21.5 million current, former, and prospective federal employees and contractors were stolen, including almost 5.6 million records with fingerprints. The incident led to a congressional investigation and the resignation of some OPM leaders.
- Thieves stole a laptop from a researcher's car that belonged to the National Institutes of Health (NIH). The laptop held the personal information of 2,500 people involved in an NIH study.
- Attackers illegally accessed the USAJOBS database and stole account and contact information. USAJOBS is the federal government's employment website. The government said that the thieves did not access sensitive personal information.
- The U.S. State Department warned 400 people about a computer security breach. The attackers stole passport application information, including Social Security numbers (SSNs). The thieves used the data to open credit card accounts.
- Spies broke into the Pentagon's computer systems. They stole data on the Department of Defense's Joint Strike Fighter aircraft.

Since 1987, the U.S. government has worked to protect federal IT systems. The first law to address federal computer security was the Computer Security Act (CSA).[4] Under the CSA,

every federal agency had to inventory its IT systems. Agencies also had to create security plans for those systems and review their plans every year.

In 2002, Congress created the Federal Information Security Management Act (FISMA).[5] It created FISMA, in part, because of the September 11, 2001, terrorist attacks in New York City and Washington, DC, which highlighted the need for better information security. FISMA recognizes that information security is crucial. It superseded most of the CSA.

Today, the Federal Information Security Modernization Act of 2014 (FISMA 2014) is the main law addressing federal government computer security protection.[6] FISMA 2014 largely superseded the 2002 act. In this book, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were not changed.

What Is Cyberwar?

On October 11, 2012, then U.S. Secretary of Defense Leon Panetta stated that attacks on the nation's critical infrastructure could be "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."[7] Many people worry about "cyberwar" or "information warfare." However, cyberwar does not take place on a physical battlefield, or on the sea or in the air. Instead, it is a conflict that takes place in or purposefully affects information systems.

The term *cyberwar* refers to conflicts between nations and their militaries. Cyberwar attacks are carried out at the direction of a particular nation. This is the main distinction between cyberwar and other types of information system attacks that are reported in the news media. Cyberwar could affect military information systems, nongovernment information systems, and private industry information systems. It includes not only threats to national security, but also threats to industry, commerce, and intellectual property. It could even include larger threats to how governments function generally. Consider these examples:

- It is believed that Russia used many different tactics, including spreading propaganda on social media, to interfere in the 2016 U.S. national elections.[8]
- The 2015 attacks on the Ukrainian power grid are largely thought to be acts of cyberwar committed by Russia.[9]
- The 2014 cyberattack against U.S.-based Sony Pictures Entertainment is believed to have been ordered by the North Korean government.[10]

Military, government, and private information systems are connected and difficult to protect. This makes defining true acts of cyberwar very difficult. The prospect of a cyberwar between nations is every bit as concerning as a conventional war. As of the writing of this book, there are no cyberwar treaties in place. Some have been introduced between various countries, and at the United Nations, but none have been adopted or ratified.

Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (New York, NY: Oct. 11, 2012). Available at: http://www.gao.gov/assets/660/652170.pdf (accessed February 4, 2014); BBC News, "Ukraine power cut was cyber attack." January 11, 2017, https://www.bbc.com/news/technology-38573074 (accessed May 16, 2020); The New York Times, "The World Once Laughed at North Korean Cyberpower. No More." October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed May 16, 2020)

This chapter focuses on how the federal government protects its IT systems and discusses many of FISMA's provisions. You should be aware that this area of law is complex and changes often.

The Federal Information Security Modernization Act

The Federal Information Security Modernization Act of 2014 recognized the complex nature of the federal computing environment.[11] It also sought to improve oversight of federal information security activities and provide a framework for making sure that information security controls are effective. This is important because the U.S. government anticipates spending over $18 billion on cybersecurity in the fiscal year 2021.[12]

Purpose and Scope

FISMA defines *information security* as protecting IT systems to provide confidentiality, integrity, and availability.[13] IT systems must be protected from unauthorized use, access, disruption, modification, and destruction.

FISMA has six main provisions. The law:

- Sets forth agency information security responsibilities
- Requires a yearly independent review of agency information security programs
- Authorizes the National Institute of Standards and Technology (NIST) to develop information security standards for IT systems that do not contain unclassified information
- Gives the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) specific oversight responsibilities
- Clarifies that national security systems (NSSs) must be secured using a risk-based approach
- Provides for a central federal security incident response (IR) center

FISMA applies to federal agencies. These agencies fall under the executive branch of the U.S. government and report to the president. Examples of federal agencies include the Federal Aviation Administration, the Social Security Administration, and the Department of Education.

FISMA also applies to contractors who perform services on behalf of a federal agency. For example, researchers at universities who work with federal agencies may have to follow FISMA requirements on their own IT systems because those systems could store federal data.

Main Requirements

FISMA has many requirements. This section will review many of them. First, this section reviews what federal agencies must do to comply with FISMA. Second, it reviews how the NIST helps agencies shape their information security programs. Third, it reviews the federal central IR center. Finally, it reviews how FISMA applies to **national security systems (NSSs)**. NSSs are IT systems that hold military, defense, and intelligence information.

Agency Information Security Programs

FISMA requires each federal agency to create an agency-wide information security program.[14] Even agencies with NSSs must create these programs. An agency's information security program must include:

- **Risk assessments**—Agencies must perform risk assessments. They must measure the harm that could result from unauthorized access to or use of agency IT systems. Agencies must base their information security programs on the results of these risk assessments.
- **Policies and procedures**—Agencies must create policies and procedures to reduce risk to an acceptable level. The policies must protect IT systems throughout their life cycle. Agencies also must create configuration management policies.
- **Subordinate plans**—Agencies must make sure that they have plans for securing networks, facilities, and systems or groups of IT systems. These plans are for technologies or system components that are a part of the larger information security program.
- **Security awareness training**—Agencies must give training to employees and any other users of their IT systems. This includes contractors. This training must make people aware of potential risks to the agency's IT systems. It also must make people aware of their duties to protect these systems.
- **Testing and evaluation**—Agencies must test their security controls at least once a year. They must test management, operational, and technical controls for each IT system.
- **Remedial actions**—Agencies must have a plan to fix weaknesses in their information security program.
- **Incident response**—Agencies must have an IR procedure. They must state how the agency detects and mitigates incidents. The procedure must include reporting incidents to the DHS United States Computer Emergency Readiness Team (US-CERT) as needed.
- **Continuity of operations**—Agencies must have business continuity plans as part of their information security programs.

An agency's information security program applies to any other organization that uses the agency's IT systems or data. An agency must protect the IT systems that support the agency's operations, even if another agency or contractor provides the systems. This can broaden the scope of FISMA, especially because IT systems and functions are often outsourced.

One of the most important parts of a FISMA information security program is that agencies test and evaluate it. FISMA requires each agency to perform "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices."[15] Agencies must test every IT system at least once a year, and test those with greater risk more often.

Agencies must also review their security controls. Some kinds of security controls are required under FISMA. The NIST has the authority to create these minimum requirements.[16] Agencies must follow the standards that NIST creates. An agency must make sure that it implements these controls properly. It must also make sure that the controls work. The yearly testing requirement recognizes that security is an ongoing process. Agencies must always monitor their information security risk. They must monitor the controls put in place to mitigate that risk as well. The head of the agency is responsible for determining the right level of risk for the agency.

Agencies must also follow NIST guidance in performing their annual reviews. If an agency uses a different model to perform its review, that model must include the same elements that NIST does. The important role of NIST is discussed later in this chapter.

NOTE

CISOs must be information security professionals and must have the "professional qualifications, including training and experience, required to administer" FISMA requirements.[19]

NOTE

CyberScope, which was created by the DHS, allows a real-time data feed that helps agencies and the OMB quickly assess the agency's information security posture.

Under FISMA, agencies must name a senior official to be in charge of information security.[17] In most agencies, this is the chief information security officer (CISO), who is responsible for FISMA compliance. The CISO's main job duties must focus on information security. Under FISMA, a CISO must have the resources necessary to make sure that the agency can comply with FISMA.

Agencies have several different reporting requirements under FISMA. For example, agencies must submit monthly electronic data feeds to the DHS through a program known as CyberScope. The purpose of these data feeds is to continuously monitor the security posture of the federal agency's information systems.

Each agency must report yearly to the OMB on its FISMA compliance activities. An agency also must send a copy of its yearly report to the following:

- House of Representatives Committee on Oversight and Government Reform
- House of Representatives Committee on Homeland Security
- House of Representatives Committee on Science and Technology
- Senate Committee on Homeland Security and Governmental Affairs
- Senate Committee on Commerce, Science, and Transportation
- U.S. Government Accountability Office (GAO)
- The agency's congressional authorization and appropriations committee[18]

An agency's FISMA report is shared widely and must be in unclassified form.[22] An agency's yearly report must review its information security program. Items reviewed must include:

- The adequacy of the program
- A description of each major information security incident experienced by the agency
- The total number of information security incidents experienced by the agency
- A description of any information security incident experienced by the agency that compromised personally identifiable information (PII).

It also must assess the agency's progress on correcting any weaknesses in the program or security controls. The agency must also respond to a set of questions about its security practices, which are asked in CyberScope. Each year the DHS publishes the questions that will be asked in the following year.

In addition to reporting on their information security activities, agencies must also report on their privacy activities. For example, they have to share information on their privacy training programs and their breach notification policy. They also must give a progress report on their efforts to eliminate the unnecessary use of SSNs and other PII.[23]

The yearly report also must include the results of an independent evaluation of the agency's information security program. Some agencies have an **inspector general (IG)**. If an agency has an IG, then the IG may carry out this evaluation. Some agencies do not have an IG. If they do not, the head of the agency must hire an external auditor to perform the evaluation.[25]

What Is an Inspector General?

An inspector general (IG) is an official who reviews the actions of a federal agency. An IG examines the agency's activities to make sure that it is operating efficiently and following good governance practices. IGs are independent officials by law. The agency that an IG reports to cannot prevent the IG from performing an audit or investigation.

The Inspector General Act of 1978 defined an IG's role.[20] An IG is responsible for:

- Conducting independent and objective audits, investigations, and inspections
- Preventing and detecting waste, fraud, and abuse
- Promoting economy, effectiveness, and efficiency
- Reviewing pending legislation and regulations
- Keeping the agency head and Congress informed about agency activities[21]

IGs are appointed to their positions based on their experience in accounting, auditing, law, and investigations. They are not political officials. Some agency heads may appoint and remove their own IGs.

The president nominates IGs for major federal agencies, and the Senate approves them. Only the president can remove these IGs. The president nominates IGs in the Department of Commerce, Department of Justice, and OMB, as well as in some other agencies.

The Role of NIST

FISMA requires the Department of Commerce to create information security standards and guidelines. The Commerce Department delegated this responsibility to NIST, an agency of the Department of Commerce. Under FISMA, NIST must create:

- Standards that all federal agencies use to categorize their data and IT systems
- Guidelines recommending the types of data and IT systems to be included in each category
- Minimum information security controls for IT systems

The OMB has stated that agencies must follow NIST standards and guidelines for non-NSSs. These standards and guidelines help agencies meet their FISMA obligations. NIST creates two different types of documents: Federal Information Processing Standards (FIPS) and Special Publications (SPs). FIPS are standards, whereas SPs are guidelines.

Federal agencies must follow FIPS. They must comply with new FIPS within 1 year of their publication date. FIPS do not apply to NSSs.

NIST creates FIPS when there is a compelling reason to do so. It creates a FIPS if there is no acceptable industry standard or solution for the underlying information security issue.

NOTE

Before CyberScope, the FISMA reporting process was time- and paper-intensive. For example, in 6 years, the Department of State produced 95,000 pages of paper to meet its FISMA reporting requirements. It spent $133 million to create these reports.[24]

NOTE

In general, a standard states mandatory actions that an organization must take to protect its IT systems. A guideline states recommended actions that an organization should follow.

As of this writing, there are 11 FIPS for information security. You can view them at https://csrc.nist.gov/publications/fips.

NIST uses procedures described in the Administrative Procedures Act (APA) to create FIPS. The APA states formal procedures for creating rules and regulations. This formal process ensures due process and makes sure that all interested agencies have a chance to comment on draft FIPS. NIST publishes a proposed FIPS in the Federal Register, which is available for public review for 30 to 90 days. The Department of Commerce must approve FIPS before they can be finalized.[26]

What Is FedRAMP?

In 2011, the United States adopted a "Cloud First" strategy as part of the Federal Government IT Modernization Act. That strategy advocated that federal agencies evaluate using cloud computing solutions for IT operations. In 2018, the U.S. federal government released its "Cloud Smart" strategy. Cloud Smart provides guidance surrounding the information security and workforce skills needed to adopt cloud computing models.[27]

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program developed by NIST, the U.S. General Services Administration, DHS, and the Department of Defense.[28] NIST also advises the FedRAMP program on FISMA compliance.

Any cloud computing services that store federal data must be FedRAMP approved. The FedRAMP program has a list of cloud computing providers that hold a FedRAMP designation. Federal agencies can purchase cloud computing services more quickly from vendors that have those designations.

FedRAMP outlines a standard approach to assess the security of cloud products and services. The FedRAMP security assessment framework is based on the NIST risk management framework (RMF). FedRAMP defines the minimum information security controls needed to safeguard cloud computing systems storing, accessing, and using federal data. Those controls are based on NIST SP 800-53, as revised.

To learn more about FedRAMP, visit https://www.fedramp.gov/.

U.S. Office of Management and Budget, "Federal Cloud Computing Strategy." Undated, https://cloud.cio.gov/strategy/ (accessed May 16, 2020); Federal Risk and Authorization Management Program, "FedRAMP Security Assessment Framework." November 15, 2017, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf (accessed May 16, 2020).

SPs are computer security guidelines that are more general than FIPS. NIST creates SPs in collaboration with industry, government, and academic information security experts. NIST does not use the very formal FIPS drafting process to create these documents.

Federal agencies have some flexibility in using the SPs for guidance. They help guide federal agencies in strengthening their IT systems. The OMB understands that this may lead to different results among federal agencies. It acknowledges that different results are expected. Agencies have no flexibility in implementing FIPS, as they are mandatory.

NIST uses a RMF approach to FISMA compliance. This framework is outlined in "SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations."[29] This approach helps protect IT systems during their whole life cycle. Federal agencies must use the RMF provided by NIST to assess the information security and privacy risks to their IT systems.

The NIST RMF outlines six steps to protect federal IT systems. They are:

1. Categorize IT systems.
2. Select minimum security controls.
3. Implement security controls in IT systems.
4. Assess security controls for effectiveness.
5. Authorize the IT system for processing.
6. Continuously monitor security controls.

NOTE

You can view the information security SPs at https://csrc.nist.gov/publications/sp800.

NIST's RMF recommends a continuous process of categorization, assessment, and monitoring. **FIGURE 8-1** shows this process.

NIST guides agencies at each RMF step. "FIPS 199, Standards for Security Categorization of Federal Information and Information Systems," helps them categorize their IT systems.[30] It serves as the starting point for an agency's information security program and helps them separate their IT systems into categories based on risk. Agencies then apply security controls to their IT system based upon their category.

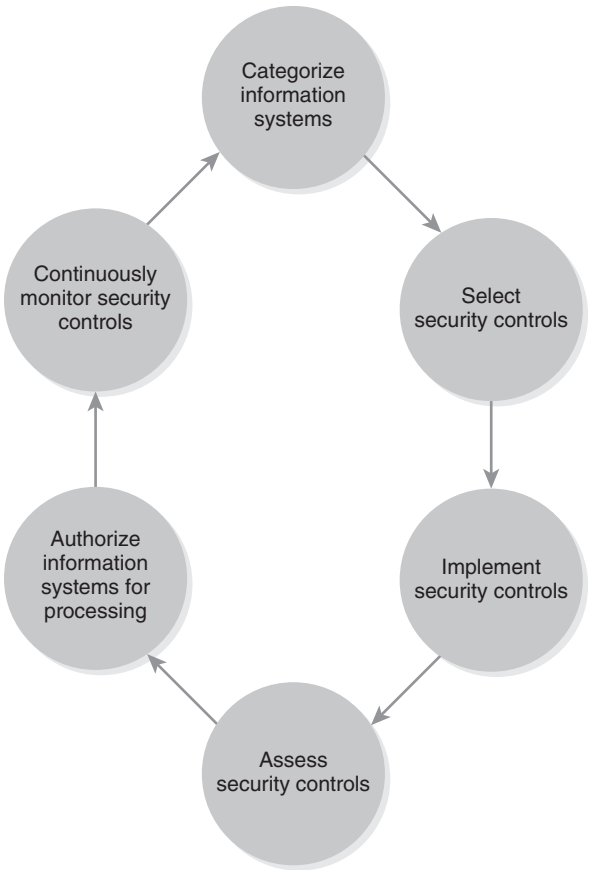

FIGURE 8-1
Risk management framework process.

Under FIPS 199, agencies must first assess the impact on IT systems because of a loss of confidentiality, integrity, or availability. The *security category* expresses that impact. FIPS defines three security categories. They are:

- **Low**—The loss of confidentiality, integrity, or availability has a limited adverse effect on the agency, its information assets, or people. A low impact event results in minor damage to assets.
- **Moderate**—The loss of confidentiality, integrity, or availability has a serious adverse effect on the agency, its information assets, or people. A moderate impact event results in significant damage to assets.
- **High**—The loss of confidentiality, integrity, or availability has a severe or catastrophic adverse effect on the agency, its information assets, or people. A high impact event results in major damage to assets.

NOTE

At the time of this writing, NIST had released a final public draft of NIST SP 800-53, Revision 5. This revision includes major enhancements to information security and privacy controls. It is anticipated that the final version of SP 800-53, Rev. 5 will be released in late 2020 or early 2021.

After the agency determines the security category, it must decide which controls to use. NIST created two documents to help with this task. They are "FIPS 200, Minimum Security Requirements for Federal Information and Information Systems"[31] and "SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations."[32] The OMB requires that agencies use these documents to make their security control decisions.

These documents require agencies to specify controls in 17 areas. FIPS 200 lists these areas. They are:

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- Risk assessment
- System and services acquisition
- System and communications protection
- System and information integrity

Agencies must apply the right security controls. They must tailor controls to the level of impact. SP 800-53 defines the minimum thresholds, or baselines, for each category. For example, agencies must use low-impact security controls in IT systems where an adverse event has a low impact. It must follow a similar practice for moderate and high impacts.

TABLE 8-1 SP 800-53 Access Control Baselines for Wireless Access

SECURITY CONTROL AREA (FIPS 200)	LOW-IMPACT SYSTEM CONTROLS (SP 800-53)	MODERATE-IMPACT CONTROLS (SP 800-53)	HIGH-IMPACT SYSTEM CONTROLS (SP 800-53)
Access control (wireless access controls)	Federal agencies must: • Establish use restrictions for wireless access, configuration requirements, and implementation guidance • Authorize wireless access to an information system before allowing access	In addition to implementing low-impact controls, the agency must also: • Protect wireless access to the system using authentication and encryption	In addition to implementing low- and moderate-impact controls, the agency must also: • Identify users allowed to configure wireless networking capabilities • Limit wireless communications to organization-controlled boundaries

TABLE 8-1 shows an example of how FIPS 200 and SP 800-53 work together. The example shows the different baselines for wireless access in the access control area.

Agencies can use other NIST guidelines to help them improve their security controls. For example, NIST has created an SP for protecting the confidentiality of PII.[33] An agency could use this SP to strengthen its access control baseline for employees that access PII. Once a federal agency has implemented security controls, it must test them.

The OMB requires federal agencies to test their security controls. "NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans" walks agencies through security control assessments.[34] These assessments are performed throughout the RMF stages.

NIST's RMF requires agencies to authorize their IT system for processing. This means that an agency must test its systems and approve its operation. This process is based on a review of the risk of operating the system. An agency must specifically accept the risks of operation before allowing an IT system to operate.

Finally, agencies must continuously monitor their security controls and make sure that they are effective. They also must document any changes to their IT systems and assess them for new risks.

Central Incident Response Center

Under FISMA, the government must have a federal IR center, which must:

- Give technical support to agencies about handling information security incidents.
- Compile and analyze data about information security incidents.
- Inform agencies about current and potential threats and vulnerabilities.
- Inform agencies about threats, vulnerabilities, and incidents to be considered as part of the agencies' risk assessment process.
- Consult with NIST and agencies with NSSs about information security incidents.[35]

NOTE

In 2018, 31 percent of the incidents reported to NCCIC/US-CERT involved employee violations of a federal agency's acceptable use policy.[36]

Agencies must report all information security incidents to the National Cybersecurity and Communications Integration Center (NCCIC). The federal IR center is also known as the US-CERT. Under FISMA, an incident is an event that

- "actually or imminently jeopardizes the integrity, confidentiality, 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."[37]

When an agency reports an incident, it must share as much information about the incident as possible. They must make reports to the NCCIC/US-CERT within 1 hour of discovering an incident that potentially compromises the confidentiality, integrity, or availability of a federal IT system.[38] An agency must share the following information about an incident when it makes a report:

- The impact the incident has had on the agency
- Whether any information has been lost, compromised, or corrupted
- The estimated amount of time and resources that are needed to recover from the incident
- When the incident was first detected
- The number of systems, records, and users impacted
- The network location of the incident
- Contact information if the NCCIC/US-CERT needs more information

The NCCIC/US-CERT coordinates IR across the U.S. government, shares information to help the government respond to threats, and also provides information security tips to the public. You can learn more at https://www.cisa.gov/securing-federal-networks.

National Security Systems

FISMA requires federal agencies to secure NSSs using a risk-based approach. An NSS includes systems that are for:

- Intelligence activities
- Command and control of military forces
- Weapons or weapons-control equipment
- Use cryptography to protect national security
- Critical to military or intelligence missions
- Must be kept classified for national defense or foreign policy[39]

FYI

FISMA does not apply to classified information. Classified information, which is protected by presidential executive order, is information that is labeled Confidential, Secret, or Top Secret. Its label is based upon its national security importance. This data must be protected to meet national security goals.

The Committee on National Security Systems (CNSS) oversees FISMA activities for NSSs. The CNSS has 21 voting members. They include officials from the National Security Administration (NSA), Central Intelligence Agency (CIA), and Department of Defense (DoD). A DoD member leads the committee. The CNSS also includes several subcommittees and panels. You can learn about the CNSS at www.cnss.gov.

Federal agencies with NSSs must follow CNSS policies. Today, CNSS policies favor following NIST guidelines and processes whenever possible.[40] However, it was not always this way. Before 2012, the CNSS often had information security policies and procedures for NSSs that were either similar to NIST guidance or very different from NIST guidance. Many commentators thought that practice caused unnecessary complexity. Today, CNSS adopts NIST guidance whenever it makes sense to do so. It only issues separate guidance when NIST guidance does not meet the information security needs of NSSs.

FISMA permits the directors of the DoD and CIA to develop additional information security policies for NSSs within their own agencies. The OMB must report to Congress on FISMA compliance for NSSs. It also makes sure that agencies with an NSS are meeting FISMA's legal requirements. The OMB makes sure that agencies with an NSS create an information security program and test it each year.

Oversight

The OMB and the DHS share responsibility for FISMA compliance. The OMB oversees FISMA-related budgetary issues. It can also withhold funding from agencies that fail to follow FISMA. In addition, the OMB must continue to issue a report to Congress each year on the government's FISMA compliance. This report details how federal agencies are complying with FISMA. It also identifies problem areas.

The DHS has had the power to ensure that agencies are meeting their FISMA obligations. It can also create rules and other guidance that these agencies must follow. These rules are called binding operational directives. The DHS also keeps track of how all federal agencies are complying with FISMA and annually reviews their cybersecurity programs. DHS also has responsibilities for governmental IR activities.

FYI

The FY2018 FISMA annual report noted that the U.S. federal government continues to have security deficiencies.[41] The top deficiencies were:

1. Lack of data protection
2. Lack of network segmentation
3. Inconsistent patch management practices
4. Lack of strong authentication
5. Lack of continuous monitoring, audit, and logging capacities.

Protecting Privacy in Federal Information Systems

Data privacy is an important issue for the federal government. There are several federal laws designed to protect data privacy. The two major laws protecting the privacy of data that the government uses in the course of business are:

- The Privacy Act of 1974[42]
- The E-Government Act of 2002[43]

The Privacy Act of 1974

Congress created the Privacy Act of 1974 to protect data collected by the government. Although it applies to records created and used by federal agencies in the executive branch, it does not apply to state or local governments.

Under the Privacy Act, a **record** is any information about a person that an agency maintains. It includes a person's educational, financial, medical, and criminal history information.[44] The act requires agencies to keep accurate and complete records. It also states that an agency should store only the data that it needs to conduct business. It should not store any extra or unnecessary data.

NOTE

The Privacy Act applies only to data collected about U.S. citizens and permanent residents.

The Privacy Act states the rules that an agency must follow to collect, use, and transfer PII. An agency cannot disclose a person's records without his or her written consent. There are 12 exceptions to this general rule.[45] If a situation falls within an exception, then the agency can disclose records without consent. An agency does not need written consent to disclose a record if the disclosure is:

- Made to a federal agency employee who needs the record to perform his or her job duties
- Required under the Freedom of Information Act
- Made for an agency's routine use
- Made to the U.S. Census Bureau to perform a survey
- Made for statistical research or reporting, and all personally identifiable data has been removed
- To the National Archives and Records Administration because the record has historical value
- Made in response to a written request from a law enforcement or regulatory agency for civil or criminal law purposes
- Made to protect a person's health or safety
- Made to Congress
- Made to the U.S. Comptroller General in the course of the performance of the duties of the U.S. Government Accountability Office
- Made in response to a court order
- Made to a consumer reporting agency for certain permitted purposes

Under the Privacy Act, a person may ask for a copy of any records that an agency has about that person.[46] The person can ask only for records that are retrievable by the person's name,

SSN, or some other type of unique identifier. A person also may ask an agency to amend any incorrect records. If an agency refuses to amend a person's record, then that person may sue the agency to have the record amended. A person also can sue the agency if it denies access to his or her records.

Federal agencies must protect the data that they collect. The Privacy Act requires them to implement administrative, technical, and physical safeguards to protect the records that they maintain. They must protect their records against any anticipated threats that could harm the people identified in the records. Under the act, harm includes embarrassment.[47]

The law requires agencies to give the public notice about their record-keeping systems. This notice is called a **system of records notice (SORN)**. An agency must publish a SORN for any system that holds records on an individual. It must publish SORNs only for systems that retrieve records either by a person's name or some other personal identifier. An agency must publish its SORNs in the Federal Register.[48]

FYI

Every agency is required to post its SORNs on its webpage. You can find the SORNs for the National Aeronautics and Space Administration (NASA) at https://www.nasa.gov/content/nasa-privacy-act-system-of-records-notices-sorns.

An agency that violates the Privacy Act can be subject to both civil and criminal penalties. A person can sue a federal agency for any Privacy Act violation. For example, people can sue if an agency denies them access to their records. They also can sue if an agency refuses to amend a record. If a court finds that an agency has intentionally or willfully violated the act, it can award a plaintiff the actual damages that he or she suffered because of the violation. Under the law, a person is entitled to recover at least $1,000.[49] A court also can order the agency to pay the plaintiff's attorney fees.

A federal agency employee can be criminally responsible for violating the Privacy Act.[50] If an employee improperly discloses information, he or she can be charged with a misdemeanor. The employee also could be fined up to $5,000. An agency employee who keeps records without filing a SORN can be fined up to $5,000.

The OMB oversees Privacy Act compliance. It can publish rules for federal agencies to follow to meet their Privacy Act responsibilities.

The E-Government Act of 2002

The E-Government Act of 2002 has privacy provisions that complement the Privacy Act. Under the E-Government Act, federal agencies must:

- Review their IT systems for privacy risks
- Post privacy policies on their websites
- Post machine-readable privacy policies on their websites
- Report privacy activities to the OMB

NOTE

A PIA is not the same as a SORN. An agency must perform a PIA any time it collects PII. However, it must post a SORN whenever that data can be retrieved using a personal identifier.

A **privacy impact assessment (PIA)** is an agency's review of how its IT systems use personal information.[51] An agency conducts a PIA to make sure that it uses personal information in a way that follows the law. The PIA also helps an agency determine the risks of collecting personal information. It also examines the types of controls that an agency must put in place to reduce privacy risks.

An agency must conduct a PIA before it develops or buys any IT system that will collect personal information. It also must perform a PIA anytime its IT systems change in such a way that new privacy risks are introduced. This includes situations where an agency changes from paper to electronic systems. An agency must conduct a PIA if it chooses to outsource an IT system or function that uses personal data.[52]

An agency's PIA must include information about its data collection practices. This information is similar to fair information practice principles. The PIA must contain the following information:

- What data the agency will collect
- Why the agency is collecting the data
- How the agency will use the data
- How the agency will share the data
- Whether people have the opportunity to consent to specific uses of the data
- How the agency will secure the data
- Whether the data collected will be a system of records defined by the Privacy Act[53]

FYI

You can read PIAs from the Federal Trade Commission at https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

An agency must submit its PIAs to the OMB. They also must make them available to the public. The only time an agency does not have to make a PIA available to the public is when doing so might compromise the security of an IT system.

The E-Government Act requires agencies to post privacy policies on their websites. The privacy policies must contain the same types of information that are in a PIA. They make the public aware of how the agency collects information. They also state how the agency uses that information.

Agencies must post a link to their privacy policies on their main website home page and write them in language that is easy to understand.

NOTE

The website for the U.S. Department of Justice is at www.justice.gov. Can you find the agency's privacy policy link on that page?

The E-Government Act also requires agencies to adopt machine-readable privacy policies. These technologies alert users about the agency's website privacy practices. A machine-readable privacy policy lets users know if the agency's privacy practices match the user's browser privacy preferences. The machine-readable

privacy policy standard is called P3P. You can read about it at http://osec.doc.gov/webresources/policies/machine_readable_privcy_policy_statements.html.

OMB Breach Notification Policy

Some states have laws, called breach notification laws or data breach laws, that require businesses and other entities to notify their customers if they suffer a security breach that discloses personal information. Some of these state laws apply to businesses operating within the state. Some also apply to state governments. These laws are discussed further in Chapter 9.

Some federal laws have breach notification provisions. For instance, the rules promulgated as part of the Health Insurance Portability and Accountability Act (HIPAA) include notification requirements. There is no government-wide federal breach notification law, although federal laws have been proposed from time to time. As of this writing, no act has yet passed Congress. A federal breach notification law would eliminate confusion over when data breaches must be reported to the public.

Over the years the OMB has released several memoranda describing breach notification requirements for federal agencies. The most recent memorandum was released in 2017.[54] It states that agencies must create a plan for notifying individuals who might be potentially affected by a breach impacting the agencies' IT systems.

The OMB defines a breach as the "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or similar occurrence" where unauthorized individuals access PII. It can also include instances where an authorized individual accesses PII for a reason that is not authorized or allowed. Under the current guidance, agencies must review the data disclosed in a breach, determine the number of individuals affected by the breach, consider the likelihood that the data is usable by unauthorized individuals, and assess the risk of harm to the people whose data is disclosed.

An agency has discretion about whether they will notify people about a breach of their PII. If an agency decides to notify individuals about a breach, they must consider:

- **Source of the notification**—The highest-ranking agency official should notify people who are affected by the breach.
- **Time for notification**—Agencies must notify the people affected by the breach without delay. An agency may delay notice only for law enforcement or national security reasons.
- **Contents of the notice**—The notice should include a description of the breach and the type of data disclosed. It should include information on how people can protect themselves from having their data used by unauthorized individuals. It also should describe what the agency is doing to mitigate the breach.
- **Means of providing the notice**—The agency must consider how to give notice to the people affected by the breach. Telephone, first-class mail, email, website postings, and release to national media outlets may all be appropriate ways to provide notice. The agency must consider the best method for a given situation. Agencies also must think about how they will give notice to individuals who are visually or hearing impaired.

The OMB memo is clear that agencies must report breaches of both paper and electronic information. You can read it at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

Import and Export Control Laws

This chapter has discussed the laws that federal agencies must follow to protect the security and privacy of information. This section talks briefly about other laws that are in place to protect the export of certain kinds of data. The United States has export control laws that limit the export of materials, data, and technical information to foreign countries. The export of some of these items is limited based on U.S. security interests. It is important to be aware that these types of laws exist. These laws are very complicated and are reviewed briefly here.

Export means the shipment of items or transmission of technology outside of the United States. It also means the transmission of technology to a non-U.S. citizen or nonpermanent resident who is located in the United States. Import and export laws are reciprocal. An export from the United States is an import to another country. A person who is bound by U.S. export control laws cannot import controlled items somewhere else. Much as the United States forbids certain products from being exported, some other countries forbid certain products from being imported.

There are three different types of export control regulations that restrict the export of certain items overseas. They also restrict the transmission of certain types of information to foreign nationals who are living in the United States. The three main regulations are:

- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- Regulations from the Office of Foreign Asset Control (OFAC)

The U.S. Department of State issues the ITAR.[55] They apply to military or defense applications and technology that does not have civil (nonmilitary or defense) uses. They are covered under export control laws because of national security concerns. For instance, the United States may want to prevent terrorists from acquiring certain types of technologies that could be used to harm the country. Any export of applications and technology covered by ITAR requires an export license, which is issued by the Department of State.

FYI

The U.S. Department of State is serious about pursuing ITAR violations. In 2017, a man was sentenced to 15 years in prison and ordered to pay over $4 million in restitution for selling U.S. Army property, including munitions, on eBay.[56]

Items that are covered by ITAR are listed on the U.S. Munitions List,[57] which is published in the Code of Federal Regulations. The list has 21 categories of different items. If an item falls within one of these categories, then it is covered by ITAR. Among the categories are guns and armament, military electronics, spacecraft, and nuclear weapons.

The penalties for violating ITAR are severe, as civil fines over $1 million are possible. The Department of State determines civil penalties.[58] ITAR violators also can be subject to criminal penalties. A person who willfully violates ITAR can be fined up to $1 million per offense. He or she also can be sentenced to up to 20 years in jail. In addition, companies that violate ITAR can be barred from selling products to the federal government.[59]

The U.S. Department of Commerce handles the EAR.[60] This responsibility is delegated to the Bureau of Industry and Security (BIS). The EAR applies to dual-use technologies, which have both military and commercial use.

NOTE

A munition is a military weapon.

Under the EAR, an exporter must have an export license for items and technologies that are on the Commerce Control List (CCL). In 2018, the BIS approved about 85 percent of these license applications.[61] The CCL has 10 broad categories. They include electronics, computers, telecommunications, and information security technologies. Some items are listed on the CCL when they are removed from the U.S. Munitions List.

Some items on the CCL cannot be exported even if a person tries to get a license to do so. Usually, this is because another law or regulation prevents it. For example, the United States has a comprehensive trade embargo against Cuba, which is the oldest U.S. embargo. An embargo is a ban against trade with another country. In this case, the government forbids almost all exports to Cuba.[62]

A person who violates the EAR can be subject to both criminal and civil penalties.[63] Violators can be fined either up to $300,000 or up to twice the value of the transaction. A person who willfully violates the EAR can be fined up to $1 million per offense. He or she also can be sentenced to up to 20 years in jail.[64]

FYI

The BIS prepares a report about export control violations. You can read the most recent report and learn more about BIS enforcement activities at https://www.bis.doc.gov/index.php/enforcement.

The Treasury Department also oversees some export laws. The Office of Foreign Assets Control (OFAC), which is part of the Treasury Department, enforces trade sanctions and embargoes. The OFAC administers trade sanctions and embargoes as part of U.S. foreign policy goals. It has the power to forbid some types of transactions based upon these goals. You can learn about the OFAC's sanctions programs at https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx.

OFAC regulations may forbid people in the United States from engaging in any trade or financial transactions with other countries. People in the United States are prohibited from engaging in trade with certain people in other countries. For example, the government prohibits trade with known terrorists or drug traffickers.

The OFAC publishes a list of individuals and companies that people in the United States are generally forbidden from dealing with. The people on this list are called *specially designated nationals (SDN)*. You can view the OFAC's SDN list at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Penalties for violating OFAC regulations are generally the same as for EAR violations.

Case Studies and Examples

The OPM is the human resources department for the U.S. federal government. Among its many responsibilities, the OPM provides background check investigation services to other federal agencies.

In 2015, the OPM announced two separate information security incidents that compromised the PII of over 21.5 million people. The incidents were caused by hackers that infiltrated OPM systems. They also infiltrated the systems of contractors used by the OPM. They had access to data for more than 6 months. It appears that the two attacks were coordinated, and some government sources suspect that the attacks were coordinated by another country.

People impacted by the breach included anyone who underwent a federal background check investigation from 2000 to 2015. The pool of affected individuals included federal employees, federal contractors, and active duty service members and veterans. It also included immediate family members and references for anyone whose information was stolen. Some of the PII exposed in the incidents included:

- SSN
- Employment history
- Education history
- Medical history (including mental health history and information about drug or alcohol abuse)
- Criminal history
- Address and address history
- Foreign travel history
- Personal information of close family members (spouse, partner, parents, siblings)

The PII stolen also included almost 5.6 million records with fingerprint data. Because of the breaches and public outcry, the OPM director and CIO resigned.

A report from the U.S. House of Representatives Committee on Oversight and Government Reform noted that the breach happened because the OPM did not prioritize its information security activities. The report also noted that the OPM did not meet many FISMA requirements.[65]

The OPM maintains a web-based resource center for victims of the 2015 incidents. The resource center includes information on the incident, frequently asked questions, and guidance for how to sign up for identity theft coverage. The OPM is required to provide that coverage through 2026 for affected individuals. You can view the resource center at https://www.opm.gov/cybersecurity/.

CHAPTER SUMMARY

This chapter reviews the laws that protect the security and privacy of data that the federal government uses. FISMA, the main law protecting the security of federal government IT systems, requires federal agencies to create information security programs. Agencies also must review their information security risks. The law requires them to implement controls to mitigate those risks.

The Privacy Act of 1974 and the E-Government Act of 2002 are the main laws protecting data privacy at the federal level. These laws govern how federal agencies use personally identifiable data. Under the E-Government Act, federal agencies must review their IT systems for any privacy impacts. Both laws require federal agencies to notify the public about their data collection practices.

KEY CONCEPTS AND TERMS

Inspector general (IG)
National security systems (NSSs)
Privacy impact assessment (PIA)
Record
System of records notice (SORN)

CHAPTER 8 ASSESSMENT

1. Which regulation controls the export of military or defense applications and technology?

A. ITAR
B. EAR
C. OFAC
D. FDIC
E. None of these is correct.

2. What information must a federal agency include in a privacy impact assessment?

3. The information collected in a PIA and a SORN is based upon what principles?

A. NIST standards
B. OMB standards
C. Fair information privacy practices
D. ITAR regulations
E. None of these is correct.

4. Which assessment must be completed any time a federal agency collects personal information that can be retrieved via a personal identifier?

A. PIA
B. SORN
C. ACORN
D. OFAC
E. None of these is correct.

5. Which agency has primary oversight responsibilities under FISMA?

A. DoD
B. CIA
C. NIST
D. CNSS
E. None of these is correct.

6. Federal agencies must report information security incidents to _____.

7. Federal agencies must test their information security controls every 6 months.

A. True
B. False

8. What are federal information security challenges?

A. A culture of merely complying with reporting requirements
B. Lack of an enterprise approach to information security
C. Lack of coordination within the federal government
D. All of these are correct.
E. None of these is correct.

9. What is the name of the FISMA data-collection tool?

10. Which type of NIST guidance follows a formal creation process?

A. Special Publications
B. Federal Information Processing Standards
C. Guidelines for Information Security
D. Fair information practice principles
E. None of these is correct.

11. How many steps are there in the NIST risk management framework?

A. Six
B. Five
C. Four
D. Three
E. None of these is correct.

12. Which level of impact for a FIPS security category best describes significant damage to organizational assets?

A. Low
B. Moderate
C. High
D. Severe
E. None of these is correct.

13. FedCIRC is the federal information security incident center.
    A. True
    B. False

14. How quickly must a federal agency report an unauthorized access incident?
    A. Monthly
    B. Weekly
    C. Daily
    D. Within 2 hours of discovery
    E. Within 1 hour of discovery

15. How many categories of security controls are designated in FIPS 200?
    A. 20
    B. 19
    C. 18
    D. 17
    E. None of these is correct.

ENDNOTES

1. Remarks by the President, "On Securing Our Nation's Cyber Infrastructure," May 29, 2009. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed May 16, 2020).
2. Committee on Oversight and Government Reform, "Federal Information Security: Current Challenges and Future Policy Considerations," March 24, 2010. http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg65549/html/CHRG-111hhrg65549.htm (accessed May 16, 2020).
3. U.S. Government Accountability Office, "Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices," July 2019. https://www.gao.gov/assets/710/700588.pdf (accessed May 16, 2020).
4. Computer Security Act of 1987, P.L. 100-235, 101 Stat. 1724.
5. Federal Information Security Management Act, Title III of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).
6. The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).
7. Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (New York, NY: Oct. 11, 2012). Available at: http://www.gao.gov/assets/660/652170.pdf (accessed May 16, 2020).
8. Time, "Here's What We Know So Far About Russia's 2016 Meddling," April 18, 2019. https://time.com/5565991/russia-influence-2016-election/ (accessed May 16, 2020).
9. BBC News, "Ukraine Power Cut Was Cyber Attack," January 11, 2017. https://www.bbc.com/news/technology-38573074 (accessed May 16, 2020).
10. The New York Times, "The World Once Laughed at North Korean Cyberpower. No More," October 15, 2017. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed May 16, 2020).
11. U.S. Code Vol. 44, sec. 3551.
12. Statista, "Proposed Budget of the U.S. Government for Cyber Security in FY 2017 to 2021," February 2020. https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ (accessed May 16, 2020).
13. U.S. Code Vol. 44, sec. 3552(b)(3).
14. U.S. Code Vol. 44, sec. 3544.
15. U.S. Code Vol. 44, sec. 3554(b)(5).
16. U.S. Code Vol. 15, sec. 278g-3.
17. U.S. Code Vol. 44, sec. 3554(a)(3).
18. U.S. Code Vol. 44, sec. 3554(c).

19. U.S. Code Vol. 44, sec. 3554(b)(3)(A)(ii).
20. Inspector General Act of 1978, U.S. Code Vol. 5 app, sec. 1.
21. Inspector General Act of 1978, U.S. Code Vol. 5 app, sec. 2.
22. U.S. Code Vol. 44, sec. 3554(c)(1)(B).
23. U.S. Office of Management and Budget, "OMB Circular A-130, Managing Information as a Strategic Resource, Section 5(f)," July 28, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf (accessed May 16, 2020).
24. Committee on Oversight and Government Reform, "Federal Information Security: Current Challenges and Future Policy Considerations," March 24, 2010. http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg65549/html/CHRG-111hhrg65549.htm (accessed May 16, 2020).
25. U.S. Code Vol. 44, sec. 3555.
26. National Institute of Standards and Technology, "Procedures for Developing FIPS (Federal Information Processing Standards) Publications," May 21, 2018. https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications (accessed May 16, 2020).
27. U.S. Office of Management and Budget, "Federal Cloud Computing Strategy," Undated. https://cloud.cio.gov/strategy/ (accessed May 16, 2020).
28. Federal Risk and Authorization Management Program, "FedRAMP Security Assessment Framework," November 15, 2017. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf (accessed May 16, 2020).
29. National Institute of Standards and Technology, "SP 800-37, Revision 1, Risk Management Framework for Information Systems and Organizations," December 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed May 16, 2020).
30. National Institute of Standards and Technology, "FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems," February 2004. https://csrc.nist.gov/publications/detail/fips/199/final (accessed May 16, 2020).
31. National Institute of Standards and Technology, "FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems," March 2006. https://csrc.nist.gov/publications/detail/fips/200/final (accessed May 16, 2020).
32. National Institute of Standards and Technology, "SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final (accessed May 16, 2020).
33. National Institute of Standards and Technology, "SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010. https://csrc.nist.gov/publications/detail/sp/800-122/final (accessed May 16, 2020).
34. National Institute of Standards and Technology, "SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 2014. https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final (accessed May 16, 2020).
35. U.S. Code Vol. 44, sec. 3556.
36. U.S. Government Accountability Office, "Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices," July 2019. https://www.gao.gov/assets/710/700588.pdf (accessed May 16, 2020).
37. U.S. Code Vol. 44, sec. 3552(b)(2).
38. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "US-CERT Federal Incident Notification Guidelines," 2017. https://www.us-cert.gov/incident-notification-guidelines (accessed May 16, 2020).
39. U.S. Code Vol. 44, sec. 3552(b)(6)(A).
40. Committee of National Security Systems, "Policy No. 22, Cybersecurity Risk Management," August 2016. http://www.cnss.gov/cnss/issuances/Policies.cfm (accessed May 16, 2020).
41. Office of Management and Budget, "Fiscal Year (FY) 2018 Annual Report to Congress," August 2019. https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf (accessed May 16, 2020).
42. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, codified at U.S. Code Vol. 5, sec. 552a.
43. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, codified in scattered sections throughout U.S. Code Vol. 44 (various sections) (2012).

44. U.S. Code Vol. 5, sec. 552a(a)(4).
45. U.S. Code Vol. 5, sec. 552a(b).
46. U.S. Code Vol. 5, sec. 552a(d).
47. U.S. Code Vol. 5, sec. 552a(e)(10).
48. U.S. Code Vol. 5, sec. 552a(e).
49. U.S. Code Vol. 5, sec. 552a(g)(4)(A).
50. U.S. Code Vol. 5, sec. 552a(i).
51. U.S. Office of Management and Budget, "Memo M-03-22: OMB Guidance for Implementing the Privacy Protections of the E-Government Act of 2002," September 26, 2003. https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/ (accessed May 16, 2020).
52. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, sec. 208.
53. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, sec. 208.
54. U.S. Office of Management and Budget, "OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf (accessed May 16, 2020).
55. International Traffic in Arms Regulations, Code of Federal Regulations, Title 22, sec. 120-130.
56. U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions Related to Criminal Cases," January 2018. https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=6ae22ec1db2a9740c53a7d321f9619c4 (accessed May 16, 2020).
57. International Traffic in Arms Regulations, Code of Federal Regulations, Title 22, sec. 121.1.
58. International Traffic in Arms Regulations, Code of Federal Regulations, Title 22, sec. 128.
59. U.S. Code Vol. 22, sec. 2778(c).
60. Export Administration Regulations, Code of Federal Regulations, Title 15, sec. 730-774.
61. U.S. Department of Commerce, "Statistics of 2018 BIS License Authorization," April 3, 2019. https://www.bis.doc.gov/index.php/documents/technology-evaluation/ote-data-portal/licensing-analysis/2453-2018-statistical-analysis-of-bis-licensing-pdf-1/file (accessed May 16, 2020).
62. U.S. Code Vol. 22, sec. 2370.
63. Export Administration Regulations, Code of Federal Regulations, Title 15, sec. 730-774.
64. U.S. Code Vol. 50, sec. 4801-4852.
65. U.S. House of Representatives, Committee Oversight and Government Reform, "The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation," September 7, 2016. https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf (accessed May 16, 2020).