CHAPTER 8

Federal Government Information Security and Privacy Regulations

IN A 2009 SPEECH, 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. He said 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. They conduct the business of running the country. They also hold sensitive security data. They 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 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 in creating information security standards
- Discuss approaches to protecting national security systems
- 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] This statistic isn't very surprising. The federal government is the largest producer and user of information in the United States.[3] Government computer systems hold data that's critical for government operations. They hold data on people living in the United States. This includes employment, tax, and citizenship data. They hold data on businesses operating in the United States. They also hold data that's used to protect the United States from threats.

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

- Thieves stole a laptop that belonged to the National Institutes of Health (NIH). They stole it from a researcher's car. The laptop held the personal information of 2,500 people involved in an NIH study.
- Hackers gained entry to Federal Aviation Administration (FAA) computers. They stole the personal information of more than 45,000 FAA employees and retirees.
- Attackers illegally accessed the USAJOBS database. USAJOBS is the federal government's employment Web site. They stole account and contact information. The government said that the thieves didn't access sensitive personal information.
- The U.S. State Department warned 400 people about a computer security breach. The attackers stole passport application information. The stolen data included 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.

The U.S. government has a history of working to protect its computers. In 1987, Congress passed the Computer Security Act (CSA).[4] This was the first law to address federal computer security. 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. The attacks highlighted the need for better information security. FISMA recognizes that information security is crucial. It superseded most of the CSA. It's now the main law that states how federal agencies must secure their IT systems.

In 2009, President Barack Obama ordered a review of cyberspace policy, which resulted in the document titled "Cyberspace Policy Review." This review looked at U.S. policies to secure government IT systems. It identified cybersecurity weaknesses. It also proposed solutions to them. After the review, President Obama identified cybersecurity as a national challenge. He said that both the federal government and private entities must focus on these issues.[6] You can read the "Cyberspace Policy Review" at *http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf.*

The review recommended that the president appoint a government cybersecurity official. This position is responsible for coordinating federal cybersecurity policies and activities. Some people call this official the "cybersecurity czar."

In March 2010, the federal CIO spoke at a House of Representatives subcommittee meeting. He talked about federal information security challenges.[7] He said the government faces the following challenges:

- Lack of coordination within the federal government
- Lack of coordination between the federal government and the private sector
- A culture within the federal government of merely complying with reporting requirements
- Lack of an enterprise approach to information technology
- Lack of focused research and development activities to enhance cybersecurity

In February 2013, U.S. President Barak Obama issued an Executive Order on cybersecurity. The purpose of the order is to improve the security of the country's critical cyberinfrastructure. Critical infrastructure means "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 or safety."[8] Critical cyberinfrastructure includes physical assets like IT systems. It also includes intangible assets like the data in those systems. Critical cyberinfrastructure isn't just government-owned IT systems and data. Almost all, nearly 90 percent, of the nation's IT critical infrastructure is actually located on private networks.[9]

To protect the nation's critical cyberinfrastructure, the order requires the government to share information with private organizations and companies. Sharing relevant data with private organizations helps those organizations protect their portions of the nation's critical cyberinfrastructure. The order also requires the government and private organizations to ensure that privacy and civil liberties protections are built into the information-sharing programs. Finally, the order specifies that the National Institute of Standards and Technology (NIST) create a cybersecurity framework to be used to protect the nation's critical infrastructure.

FYI

The first version of the NIST Framework for Improving Critical Infrastructure Cybersecurity was released in February 2014. You can read more about the framework at *http://www.nist.gov/cyberframework*.

On October 11, 2012, the Secretary of Defense 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."[10] Many people worry about a "cyberwar" or "information warfare." Cyberwar doesn't take place on a physical battlefield, or on the sea or in the air. Instead, it's conflict that takes place in or purposefully affects information systems. 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 also even include attacks that compromise social networks and personally identifiable information.

The term *cyberwar* specifically refers to conflicts between nations and their militaries. This is the main distinction between cyberwar and other types of information system attacks that are reported in the news media. Military, government, and private information systems are connected and difficult to protect. 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.

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. In the past couple of years, new FISMA compliance tools have been introduced. Now federal agencies can report on FISMA activities in near real time. In July 2010, the Department of Homeland Security became responsible for collecting metrics on how federal agencies comply with FISMA.[11] Agencies with FISMA responsibilities are starting to work together to create a government-wide information security risk management structure. It is probable that the laws that affect federal IT systems and other parts of the national critical infrastructure will continue to evolve.

The Federal Information Security Management Act

President George W. Bush signed the Federal Information Security Management Act in 2002. It's part of the E-Government Act of 2002. FISMA is Title III of the E-Government Act.

FISMA merges a number of different laws.[12] All of these laws addressed different information security issues. Since no one law was comprehensive, Congress heard many reports that information security efforts at the federal level were not effective. Congress intended FISMA to be a strong law to fix this problem. It would guide federal agencies in making sure that their IT systems are secure.

Purpose and Scope

Congress created FISMA to protect federal IT systems and the data in those systems. FISMA defines *information security* as protecting IT systems in order 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 NIST to develop information security standards for IT systems that do not contain unclassified information
- Gives the OMB specific oversight responsibilities, some of which were transferred to the DHS in July 2010
- Clarifies that national security systems (NSSs) must be secured using a risk-based approach
- Provides for a central federal security incident response center

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

Main Requirements

FISMA has many requirements. This section will review most of them. First, this section reviews what federal agencies must do to comply with FISMA. Second, it reviews how NIST helps agencies shape their information security programs. Third, it reviews the federal central incident response center. Finally, it reviews how FISMA applies to **national security systems**. National security systems 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.
- **Annual inventory**—Agencies must inventory their IT systems. They must update that inventory each year.

- **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 its information security program.
- **Incident response**—Agencies must have an incident response procedure. They must state how the agency detects and mitigates incidents. The procedure must include reporting incidents to the Department of Homeland Security 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. It must protect them even if another agency or contractor provides the systems. This can broaden the scope of FISMA, especially since IT systems and functions are often outsourced.

FISMA 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. That's because those systems could store federal data. The OMB has required that FISMA security requirements be included in research grants where applicable.[15]

FYI

In January 2008, the NIH said that FISMA applies to NIH grants when a researcher collects, stores, processes, or uses data on behalf of the Department of Health and Human Services (HHS). The NIH is a part of HHS. You can read the notice at *http://grants.nih.gov/grants/guide/notice-files/NOT-OD-08-032.html.*

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."[16] Agencies must test every IT system at least once a year. They must test IT systems with greater risk more often.

Agencies must also review their security controls. Some kinds of security controls are required under FISMA. NIST created security standards to help implement the controls that FISMA requires. Agencies must follow these standards. These standards specify minimum security controls. An agency must make sure that they implement 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 role of NIST is discussed later in this chapter.

Under FISMA, agencies must name a senior official to be in charge of information security. In most agencies, this is the chief information security officer (CISO). The CISO 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.

NOTE

CISOs must be information security professionals. They must have the "professional qualifications, including training and experience, required to administer" FISMA requirements.[18]

Agencies have a number of different reporting requirements under FISMA. For example, some large agencies must submit monthly electronic data feeds to the DHS. These data feeds are submitted 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. Small federal agencies don't have to submit monthly reports. However, the OMB strongly encourages them to do so anyway.[17]

NOTE

CyberScope was created by the Department of Homeland Security. The tool allows a real-time data feed that helps agencies and the OMB quickly assess the agency's information security posture.

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

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

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's operating efficiently and following good governance practices. IGs are independent officials by law. The agency that an IG reports to can't prevent the IG from performing an audit or investigation.

The Inspector General Act of 1978 defined an IG's role.[19] 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

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

The president nominates IGs for major federal agencies. 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.

An agency's FISMA report is shared widely. The OMB has said that agencies shouldn't include too much information about actual IT system operations in their reports. It's possible that criminals could learn about weaknesses in IT systems by reading the reports.

An agency's yearly report must review its information security program. 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. These questions are asked in CyberScope. Each year the DHS publishes the questions that will be asked in the following year.[20]

In addition to reporting on their information security activities, agencies must also report on their privacy activities. In 2014, agencies will 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 Social Security Numbers and other personally identifiable information.[21]

NOTE

Prior to CyberScope, the FISMA reporting process was time and paper intensive. For example, in six 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.[22]

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 don't have an IG. If they don't, the head of the agency must hire an external auditor to perform the evaluation.[23]

Agencies can also be interviewed about their FISMA compliance status. These interviews are conducted by the DHS. The interviews include the agency's Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The goals of the interview are to:

- Gauge the agency's progress toward FISMA compliance
- Raise awareness of FISMA reporting requirements and security best practices
- Establish face-to-face communication with the agency's leaders

You can read the OMB's 2013 FISMA report instructions at *https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2014/m-14-04.pdf.*

The Role of NIST

> **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.

FISMA requires the Department of Commerce to create information security standards and guidelines. The Commerce Department delegated this responsibility to NIST. NIST is 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-national security systems. These standards and guidelines help agencies meet their FISMA obligations. NIST creates two different types of documents. They are Federal Information Processing Standards (FIPS) and Special Publications (SPs). FIPS are standards. SPs are guidelines.

Federal agencies must follow FIPS. They must comply with new FIPS within one year of their publication date. FIPS don't apply to national security systems.

NIST creates FIPS when there's a compelling reason to do so. It creates a FIPS if there's no acceptable industry standard or solution for the underlying information security issue. As of this writing, there are 17 FIPS for information security. You can view them at *http://csrc.nist.gov/publications/PubsFIPS.html.*

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. It makes sure that all interested agencies have a chance to comment on draft FIPS. NIST publishes a proposed FIPS in the Federal Register.

FISMA Implementation Project

NIST created a FISMA Implementation Project to help it meet its FISMA duties. The project helped it create FISMA-related standards and guidelines in a timely manner. The project had two phases. In the first phase, NIST developed standards and guidelines to help agencies meet basic FISMA requirements. The documents developed in this phase helped agencies create their information security programs. Phase I lasted from 2003 to 2012.[25]

In Phase II of the project, NIST created additional guidance materials. These materials helped organizations fine-tune their information security programs. This phase took place from 2007 to 2012.

It takes time to create thoughtful guidance and standards. NIST consulted with many different sources when it created guidance. It also updated its guidelines and standards frequently. You can learn more about the FISMA Implementation Project at *http://csrc.nist.gov/groups/SMA/fisma/overview.html.*

A proposed FIPS is available for public review for 30 to 90 days. The Department of Commerce must approve FIPS before they can be finalized.[24]

Special Publications are computer security guidelines. They are more general than FIPS. NIST creates SPs in collaboration with industry, government, and academic information security experts. NIST doesn't use the very formal FIPS drafting process to create these documents.

NOTE

You can view SPs at *http://csrc.nist.gov/publications/PubsSPs.html.*

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 risk management framework (RMF) approach to FISMA compliance. This framework is outlined in "SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."[26] This approach helps protect IT systems during their whole life cycle. 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.

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.[27] It serves as the starting point for an agency's information security program. It helps them separate their IT systems into categories based on risk. Agencies then apply security controls to their IT system based upon their category.

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

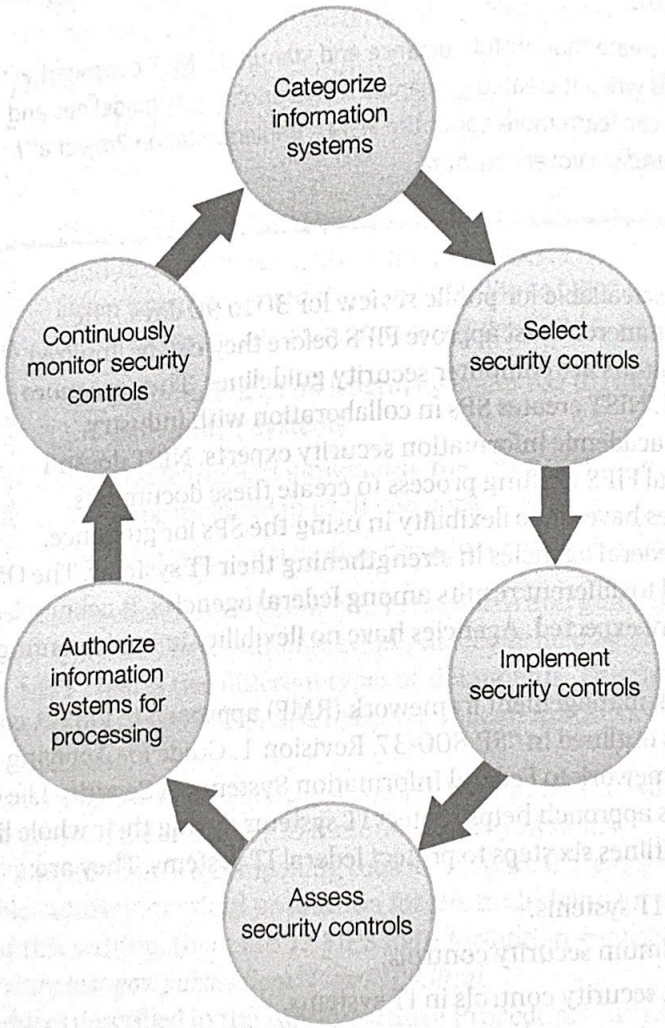

FIGURE 8-1
Risk management framework process.

- **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.

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"[28] and "SP 800-53, Revision 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations."[29] 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)	The agency must: • Establish use restrictions for wireless access, configuration requirements, and implementation guidance • Authorize wireless access to an information system prior to 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 a SP for wireless network access authentication.[30] An agency could use this SP to strengthen its access control baseline. Once it has implemented security controls, it must test them.

The OMB requires federal agencies to test their security controls. "NIST SP 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations" walks agencies through security control assessments.[31] 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 their systems and approve their operation. This process is based on a review of the risk of operating the system. An agency must specifically accept the risks of operation prior to allowing an IT system to operate.

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

The RMF and NIST supporting documents for each step are listed in Table 8-2.

NIST's Risk Management Framework

You should note that the RMF in SP 800-37, Revision 1, is relatively new to federal agencies. NIST updated this document in February 2010. Prior to 2010, this SP was called "Guide for Security Certification and Accreditation."

The OMB requires federal agencies to certify their IT systems. They also must accept the risk of running the systems. This process used to be known as *Certification and Accreditation*, or C&A. Agencies used the old version of NIST SP 800-37 to complete a C&A. Some FISMA references still refer to the C&A process. This process is now called *security authorization*. You may hear references to the old terms for quite some time.

NIST and the OMB realized that the C&A process had some problems. Some agencies thought that it was merely a compliance exercise. They didn't review their IT systems in a comprehensive manner. The new RMF and security authorization process shows that C&A is more than just planning for IT systems. It also includes continuous testing and monitoring of those systems. C&A is now one part of the RMF process.

The new RMF also is notable because NIST worked on it with many other federal agencies. This group was called the Joint Task Force Transformation Initiative Interagency Working Group. NIST and members of the intelligence, military, and national security communities were part of the group. The group created a common framework for information security management throughout the federal government.

The new RMF signals changes in FISMA compliance. It's becoming more thorough. It makes information security an ongoing and evolving process, rather than a documentation exercise.

TABLE 8-2 Risk management framework and NIST supporting documents.

RISK MANAGEMENT FRAMEWORK STEP	NIST SUPPORTING DOCUMENTATION
Categorize IT systems	FIPS 199, Security categorization
	SP 800-60, Security category mapping
Select minimum security controls	FIPS 200, Minimum security controls
	SP 800-53, Security and privacy controls
Implement security controls in IT systems	SP 800-70, Checklist for IT products
Assess security controls for effectiveness	SP 800-53A, Guide to assessing controls
Authorize the IT system for processing	SP 800-37, Risk management framework
Continuously monitor security controls	SP 800-37, Risk management framework
	SP 800-53A, Guide to assessing controls

Central Incident Response Center

Under FISMA, the government must have a federal incident response (IR) center. The OMB is responsible for this. Under FISMA, the IR center must:

- Give technical support to agencies about information security incidents.
- Share information about security incidents.
- Inform agencies about current and potential threats and vulnerabilities.
- Consult with NIST and agencies with national security systems about information security incidents.

> **NOTE**
> From 2006 to 2012, the number of incidents reported by federal agencies to the US-CERT increased by 782 percent.[32]

NIST created a national IR center in 1996. It was called the Federal Computer Incident Response Capability (FedCIRC). In 2003, the DHS was given the responsibility to run a federal IR center. The FedCIRC was absorbed into the DHS center. It's now called the US-CERT. US-CERT is part of National Cybersecurity and Communications Integration Center (NCCIC). NCCIC is operated by the DHS.

Agencies must report all information security incidents to the US-CERT. This includes NSS incidents. An incident is a violation of computer security policies or practices. It also includes an imminent threat of violation of policies or practices. The government's incident categories are:

- **Category 0: Exercise/Network Testing**—This category is for internal testing activities. These incidents aren't reported. This category is only for internal agency use.
- **Category 1: Unauthorized Access**—Agencies must report unauthorized access to their IT systems in this category. Unauthorized access is technical or physical access to an IT system. An agency must report these incidents even if data isn't compromised.
- **Category 2: Denial of Service (DoS)**—An agency must report successful DoS attacks that harm its IT systems.
- **Category 3: Malicious Code**—An agency must report successful installation of malicious software on its IT systems. They don't have to report attempted attacks stopped by antivirus software.
- **Category 4: Improper Use**—Agencies must report violations of their acceptable use policies.
- **Category 5: Scans, Probes, and Attempted Access**—Agencies must report any activities that seek to access or identify its IT systems. These activities aren't compromises or DoS attacks.
- **Category 6: Investigation**—This category is for unusual events. These incidents require more review because they're odd or potentially harmful. These incidents aren't reported. This category is only for internal agency use.

Agencies must report incidents within certain timeframes. Table 8-3 lists when agencies must report incidents to the US-CERT.

TABLE 8-3 Federal agency incident reporting timeframe.

CATEGORY	REPORTING TIMEFRAME
Category 0—Exercise/Network Defense Testing	None
Category 1—Unauthorized Access	Within one hour of discovery
Category 2—DoS	Within two hours of discovery if the attack is ongoing and the agency isn't able to stop it
Category 3—Malicious Code	Daily; must be reported within one hour of discovery if widespread across an agency
Category 4—Improper Use	Weekly
Category 5—Scans, Probes, and Attempted Access	Monthly; must be reported within one hour of discovery if an IT system contains classified information
Category 6—Investigation	None

The US-CERT coordinates IR across the government. It shares information to help the government respond to threats. It also provides information security tips to the public. You can learn more about US-CERT at *http://www.us-cert.gov.*

National Security Systems

FISMA requires federal agencies to secure national security systems using a risk-based approach. A 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

FYI

FISMA doesn't apply to classified information. Classified information is protected by presidential executive order. It's information that's 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. "National Security Directive 42" (NSD-42) gives the CNSS this authority. NSD-42 defines the roles and responsibilities for securing national security systems. President George H. W. Bush signed it in 1990. The CNSS reports to the President on the security status of these systems. In 2001 the CNSS was named a standing committee as part of the President's Critical Infrastructure Protection Board.[33]

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 a number of subcommittees and panels. You can learn about the CNSS at *www.cnss.gov*.

Federal agencies with NSSs must follow CNSS policies. In January 2012, the CNSS updated "Policy No. 22, Information Assurance Risk Management Policy for National Security Systems."[34] It outlines a six-step process for protecting NSSs. All agencies with a NSS must follow it. This framework is the same as the NIST RMF. They're similar because NIST and the CNSS worked together on a joint task force to create them.

Access Control Models

An access control model is an information security control. Security controls are built into operating systems and applications. They're used to control how people access files and data in an IT system. They're automated controls. There are three main types of access control models:

- **Discretionary access control (DAC)**—In this model, a data owner decides which subjects can access certain resources. DAC models are based on the identity of the subject seeking access to a resource. In this model, data owners have a lot of freedom to decide who can access files or data.
- **Mandatory access control (MAC)**—In this model, data owners don't have the ability to decide who can access certain files or data. This model is based on a security label system. Users of the system have a security label. Data and files in the system also have a security label. A user can access only data with the same (or lower) security label.
- **Role-based access control (RBAC)**—In this model, users are assigned roles in a system. They can access only data that is associated with their role. A person can't access data that isn't associated with his or her role.

DAC and RBAC models are usually found in industry. RBAC models, in particular, allow businesses flexibility in allowing access to data. MAC systems usually are associated with the military and classified data. This is because these systems place a high value on confidentiality.

You may also hear the term *rule-based access control*. Rule-based access control is a technique used to support different access control models. These rules are defined by an organization's security policy.

NIST and CNSS also worked together to standardize how agencies categorize IT systems. They created similar processes for choosing information security controls. CNSS "Instruction No. 1253, Security Categorization and Control Selection for National Security Systems" lists security controls for NSSs.[35] This document is an NSS-focused companion to NIST "SP 800-53, Recommended Security Controls For Federal Information Systems."

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 a NSS are meeting FISMA's legal requirements. The OMB makes sure that agencies with a NSS create an information security program and test it each year.

Oversight

Prior to July 2010, the OMB was responsible for overseeing FISMA compliance. Some of this responsibility was transferred to the DHS at that time. The OMB will still oversee FISMA-related budgetary issues. The OMB 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.

Since July 2010, 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. It also keeps track of how all federal agencies are complying with FISMA and annually reviews their cybersecurity programs. It retains its prior responsibilities with respect to incident response.

The OMB and DHS share some FISMA oversight with other agencies, particularly with respect to national security systems. The Directors of the DoD and CIA also have some FISMA oversight responsibilities. The DoD has responsibility for NSSs that hold military information. The CIA has responsibility for NSSs with intelligence information.

Protecting Privacy in Federal Information Systems

Data privacy is an important issue for the federal government. There are a number of 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[36]
- The E-Government Act of 2002[37]

The Privacy Act of 1974

Congress created the Privacy Act of 1974[38] to protect data collected by the government. It applies to records created and used by federal agencies in the executive branch. It doesn't apply to state or local governments.

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

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.[39] 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 shouldn't store any extra or unnecessary data.

The Privacy Act states the rules that an agency must follow to collect, use, and transfer personally identifiable information. An agency can't disclose a person's records without his or her written consent. There are 12 exceptions to this general rule.[40] If a situation falls within an exception, then the agency can disclose records without consent. An agency doesn't 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.[41] 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 indentified in the records. Under the act, harm includes embarrassment.[42]

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.

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 due to the violation. Under the law, a person is entitled to recover at least $1,000.[43] 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.[44] 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 compliment the Privacy Act. Under the E-Government Act, federal agencies must:

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

A **privacy impact assessment (PIA)** is an agency's review of how its IT systems use personal information.[45] 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.

NOTE

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

FYI

Every agency is required to post its SORNs on its Web page. You can find the SORNs for the National Aeronautics and Space Administration (NASA) at *http://www.nasa.gov/privacy/nasa_sorn_index.html*.

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.[46]

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[47]

An agency must submit its PIAs to the OMB. They also must make them available to the public. The only time an agency doesn't 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 Web sites. 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 Web site home page. They must write them in language that is easy to understand.

The E-Government Act also requires agencies to adopt machine-readable privacy policies. Agencies had to implement them by the end of 2004. These technologies alert users about the agency's Web site 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.*

NOTE

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

OMB Breach Notification Policy

Some states have laws that require businesses and other entities to notify their customers if they suffer a security breach that discloses personal information. These laws are called breach notification laws or data breach laws. Many states have them.[48] Some of these state laws apply to businesses operating within the state. Some also apply to state governments.

Some federal laws have breach notification provisions. For instance, recent amendments to the Health Insurance Portability and Accountability Act (HIPAA) include notification requirements. There's no government-wide federal breach notification law. Following the well-known Target credit card compromise in 2013, however, there has been more public support for a federal breach notification law.[49] A federal breach notification law would eliminate confusion over when data breaches must be reported to the public.

In May 2007, the OMB required all federal agencies to create a breach notification plan. The OMB issued this instruction in response to a large data breach at the Department of Veterans Affairs.[50] It stated that agencies must consider the following items when creating a breach notification plan:

- **Whether breach notification is required**—Agencies must review the data disclosed in a breach. They must determine the number of individuals affected by the breach. They must consider the likelihood that the data is usable by unauthorized individuals. They must assess the risk of harm to the people whose data is disclosed.
- **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.
- **Source of the notification**—The highest-ranking agency official should notify people who are affected by the breach.
- **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, e-mail, Web site 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.
- **Who gets the notice**—The agency must consider who must be notified. The people affected by the breach must be notified. In addition, the agency also must consider whether it should notify the media or other people who might be affected by the breach or the notification.

The OMB memo was very clear that agencies must report breaches of both paper and electronic information. You can read it at *https://www.bia.gov/cs/groups/xocio/documents/text/idc-041032.pdf.*

The OMB also wanted agencies to take steps to limit the amount of data that they collect. It wanted them to limit data collection so that there's less chance that personal data could be compromised in a breach. The OMB breach notification memo also required federal agencies to:

- Review and reduce the volume of personally identifiable information that they store
- Eliminate unnecessary use of SSNs and explore alternatives to using an SSN as a personal identifier
- Develop policies and procedures for individuals who are authorized to access personally identifiable information

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's 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 non-permanent 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 can't 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. They 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.[51] They apply to military or defense applications and technology that doesn't have civil (non-military or defense) uses. Any export of applications and technology covered by ITAR requires an export license. The Department of State issues the export license.

FYI

The U.S. Department of State is serious about enforcing ITAR. In 2006, the Boeing Company agreed to pay a $15 million fine to settle allegations that it violated ITAR. You can read about that case at *http://www.pmddtc.state.gov/compliance/consent_agreements/BoeingCompany.html.*

Items that are covered by ITAR are listed on the U.S. Munitions List.[52] This list 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's covered by ITAR.

The penalties for violating ITAR are severe. Civil fines up to $500,000 are possible. The Department of State determines civil penalties. 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 10 years in jail. Companies that violate ITAR can be barred from selling products to the federal government.[53]

The U.S. Department of Commerce handles the EAR.[54] This responsibility is delegated to the Bureau of Industry and Security (BIS). The EAR apply to dual-use technologies. These technologies have both a military and a commercial use. They may be covered under export control laws because of national security concerns. In 2009, the government began a review of the export control system. The purpose of the review is to ensure that the U.S. Munitions List and EAR are modernized.[55]

Under the EAR, an exporter must have an export license for items and technologies that are on the Commerce Control List (CCL). The CCL has 10 categories. They include electronics, computers, telecommunications, and information security technologies. Some items on the CCL can't be exported even if a person tries to get a license to do so. For example, the United States has a comprehensive trade embargo against Iran. An embargo is a ban against trade with another country. The government forbids almost all exports to Iran.[56]

A person who violates the EAR can be subject to both criminal and civil penalties. Violators can be fined either up to $250,000 or up to twice 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.[57]

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.*