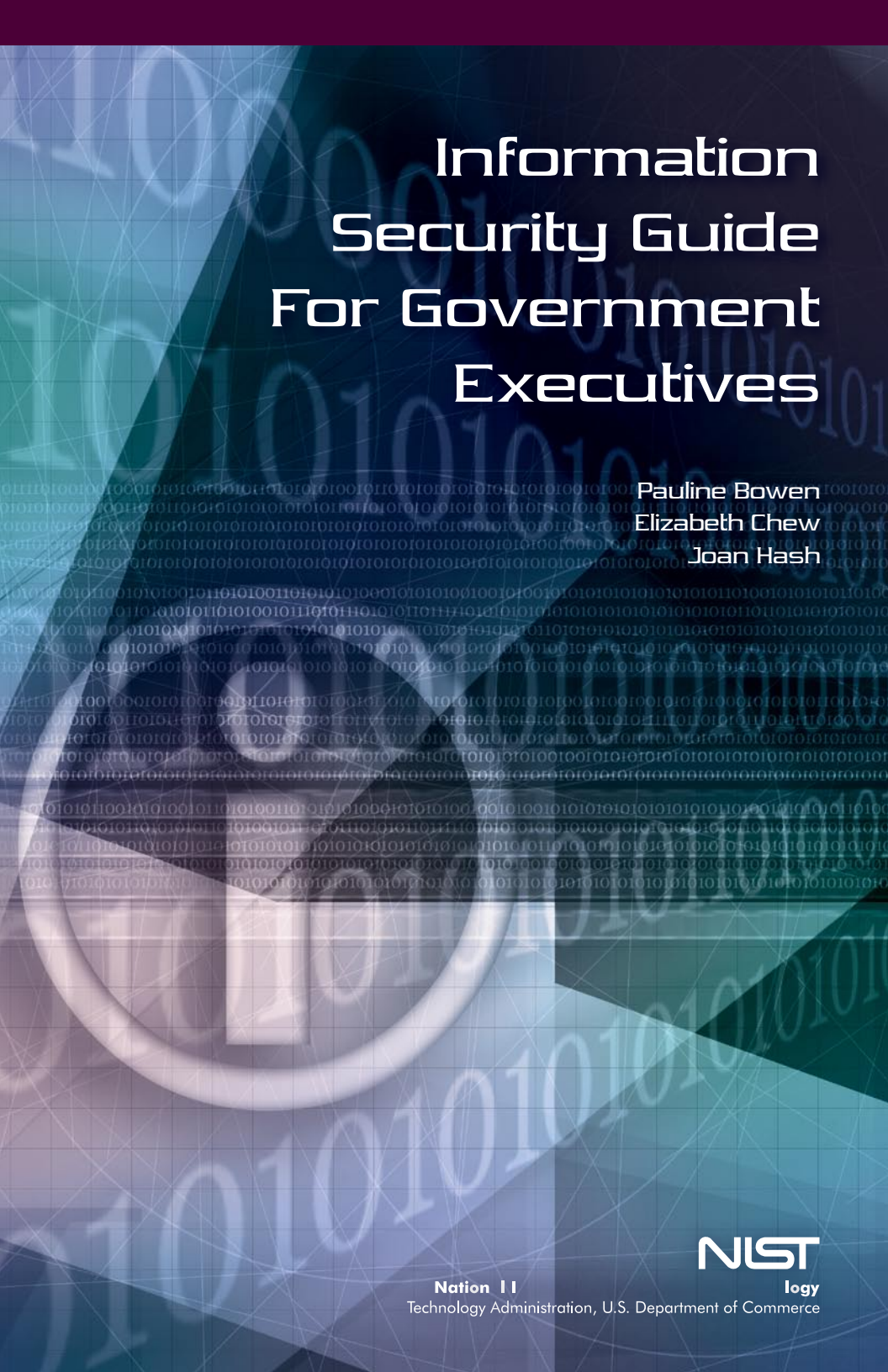

Information Security Guide For Government Executives

Pauline Bowen
Elizabeth Chew
Joan Hash

NIST
Nation l l logy
Technology Administration, U.S. Department of Commerce

Table of Contents

Introduction	1
Why do I need to invest in information security?	2
Where do I need to focus my attention in accomplishing critical information security goals?	4
What are the key activities to build an effective information security program?	6
What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective security program?	10
Where can I learn more to assist me in evaluating the effectiveness of my information security program?	14

Introduction

Information Security for Government Executives provides a broad overview of information security program concepts to assist senior leaders in understanding how to oversee and support the development and implementation of information security programs. Senior management is responsible for:

- Establishing the organization's information security program;
- Setting program goals and priorities that support the mission of the organization; and
- Making sure resources are available to support the information security program and make it successful.

Senior leadership commitment to information security is more important now than ever before. Studies have shown that senior management's commitment to information security initiatives is the single most critical element that impacts an information security program's success.

Organizational assets and operations have become increasingly dependent on information and technology to accomplish mission and performance goals. Recognizing this dependency, information becomes a strategic enabler for mission accomplishment; therefore, protecting that information becomes a high priority of an organization. Meeting this need necessitates senior leadership focus on effective information security governance and support, which requires integration of security into the strategic and daily operations of an organization. When considering this challenge, several key security questions emerge for the executive. This document will answers these questions and provides strategies to aid senior leaders in implementing an effective information security program.

1. Why do I need to invest in information security?
2. Where do I need to focus my attention in accomplishing critical information security goals?
3. What are the key activities to build an effective information security program?
4. What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective security program?
5. Where can I learn more to assist me in evaluating the effectiveness of my information security

WHY DO I NEED TO INVEST IN INFORMATION SECURITY?

Achieving compliance with information security laws, regulations, standards, and guidance is imperative for an effective information security program. To be successful, executives need to understand how to systematically recognize and address information security risks and take steps to understand and manage these risks through their information security program. Information and information systems serve as a fundamental enabler for Federal agencies to meet their primary objective of serving the American public—making the confidentiality, integrity, and availability of information paramount to the Federal government's ability to deliver services to the American public. Information security should be closely aligned with business or mission goals. The cost of protecting information and information assets should not exceed the value of the assets. To properly align business risks and information security, management should facilitate a cooperative discussion between business units and information security managers.

Information security program implementations often suffer from inadequate resources—management commitment, time, money, or expertise. By understanding the benefits of meeting compliance objectives, an organization can overcome these obstacles and appreciate the gains achieved through implementing effective security practices.

Investment in information security has many benefits. These benefits include:

- **Business success/resilience.** Effective security ensures that vital services are delivered in all operating conditions. Information is one of the most important assets to an organization. Ensuring the confidentiality, integrity, and availability of this strategic asset allows organizations to carry out their missions.

- **Increased public confidence and trust.** Proactively addressing security can be used to build good public relations – communicating to constituents the organization's focus and priority on protecting their sensitive information.

- **Performance improvements and more effective financial management.** Specific performance gains and financial savings are realized by building security into systems as they are developed, rather than adding controls after the systems are operational—or in a worst case, after an organization has had a security breach or incident.

- **Executives may be held accountable.** Federal executives may face administrative and/or legal actions for not complying with security mandates. Security is ultimately the responsibility of executive leaders such as agency heads and program officials.

- **E-government goals and objectives can be realized, leading to an improved ability to deliver products and services electronically.** Effective security provides for the integrity and availability necessary to meet demanding customer service requirements.

- **Security is integrated within your business processes to protect your information and the assets that support your agency.** Leaders should deploy proactive security to enable mission delivery and enhance value to the organization, rather than view it as an afterthought or as a reactionary mechanism to legislation, regulation, and oversight.

- **Risk management practices mature and become an integral part of doing business.** The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Therefore, the risk management process should be treated as an essential management function of the organization, rather than a technical function carried out by system administrators.

- **Decreased risk to operations and business.** Real risks to operations can be brought on through a variety of sources, in some cases resulting in damage to infrastructure and the complete shutdown of E-government services. For example, loss of all Internet connectivity, denial of service attacks, and environmental factors (e.g., power outages, floods, fires) can result in a loss of availability of key information, rendering an organization unable to deliver on its mission. Investment in security can assist in mitigating risks to operations, business and the organization mission.

Over time, information security efforts may need to be revisited because of changes in agency mission, operational requirements, threats, environment, or deterioration in the degree of compliance. Periodic assessments and reports on activities can be a valuable means of identifying areas of noncompliance. Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment. Executives should ensure a life-cycle approach to compliance by monitoring the status of their programs to ensure that:

- Ongoing information security activities are providing appropriate support to the agency mission;

- Policies and procedures are current; and

- Security controls are accomplishing their intended purpose.

WHERE DO I NEED TO FOCUS MY ATTENTION IN ACCOMPLISHING CRITICAL INFORMATION SECURITY GOALS?

Implementing a robust information security program within the federal government is challenging. Federal executives have to contend with constantly changing technology, multiple compliance requirements, increasing complexity of information security, and changing threats. However, the executive can navigate these challenges and accomplish an organization's critical information security goals. The following points are critical to executives' success in accomplishing information security goals:

- **Strong leadership is the foundation to build a successful information security program.** Executive leadership demonstrates an active commitment to the information security program. This requires visible participation and action; ongoing communication and championing; and placing information security high on their agenda. Executives must serve as role models in placing a high priority on information security and in setting the stage for an organization's approach to implementing a program and setting expectations for improved security performance.

- **Good business practices lead to good security.** Effective business management in the federal government should focus on delivering services to the American people. Executives must align strategic information security initiatives with an agency's mission and integrate information security into all business goals, strategies, and objectives.

- **Be proactive vs. reactive.** Information security programs need to be developed and implemented based upon effective risk management processes. Weaknesses and vulnerabilities must be resolved – executives should ensure that the overall programmatic focus remains on proactive security and the prevention of tomorrow's problems.

- **Develop stakeholders/support within the executive ranks and focus their efforts on collaboration and cooperation vs. stovepipes and competition.** By leveraging support within the executive ranks, security can be increasingly viewed from an enterprise perspective. Sharing responsibility for security facilitates integration of security into agency business and strategic planning processes in a consistent and holistic manner.

- **People can make or break your program.** Solving the information security dilemma through people starts with obtaining the right talent to execute the program. Leadership should be committed to staffing the information security program with appropriate resources. Once staff have been identified and committed to the efforts, leadership needs to actively and publicly assign responsibility and authority to execute the program. Staff will need to be trained on their responsibilities and maintain an ongoing baseline of knowledge appropriate to their responsibilities. It is important to invest in the retention of information security staff, including your entire management team (CIO, SAISO/CISO, etc.), program managers, and information security workforce, who are key to the success of the information security program.

- **Information security program development is comprehensive and takes time to accomplish.** Executives, as leaders, should appreciate the ongoing efforts needed to develop, implement and maintain an effective program. While specific tasks can and will have specific timelines for completion, it is imperative that at their conclusion the executive openly recognizes the importance of the ongoing security lifecycle. The executive should recognize that each organization will have unique characteristics and complexities that will dictate the time and level of effort required to reach each organizations' milestones.

WHAT ARE THE KEY ACTIVITIES TO BUILD AN EFFECTIVE INFORMATION SECURITY PROGRAM?

Successful information security programs must be developed and tailored to the specific organizational mission, goals, and objectives. However, all effective security programs share a set of key elements. NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, provides guidance on the key elements of an effective security program summarized below along with a reference of applicable NIST security documents. These individual program elements must be integrated through the following common activities:

- Establishing effective governance structure and agency-specific policy;
- Demonstrating management support to information security; and
- Integrating the elements into a comprehensive information security program.

INFORMATION SECURITY PROGRAM ELEMENTS	
Security Planning	Security planning begins at the enterprise or organization level, and filters all the way down to the system level. It is imperative to create an organizational infrastructure that supports security planning, positioning the appropriate staff into key roles, including, but not limited to, the: ◆ Chief Information Officer (CIO); ◆ Senior Agency Information Security Officer (SAISO) or Chief Information Security Officer (CISO); ◆ Information System Owner; ◆ Information Owner; ◆ Information System Security Officer; and ◆ Authorizing Official NIST SP 800-100, *Information Security Handbook, A Guide for Managers, Chapter 8 Security Planning* FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
Capital Planning	Federal agencies are required to follow a formal enterprise capital planning and investment control (CPIC) process designed to facilitate and control the expenditure of agency funds. Increased competition for limited federal budgets and resources requires that agencies allocate available funding toward their highest priority information security investments. FISMA and other existing federal regulations enforce this practice by instructing federal agencies to integrate information security activities and the CPIC process. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
Awareness and Training	The security awareness and training program is a critical component of the information security program. It is the vehicle for disseminating security information that the workforce, including managers, needs to do their jobs. These programs will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information resources entrusted to them. **Awareness** is a blended solution of activities that promotes security, establishes accountability, and informs the workforce of security news. **Training** strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role. **Education** integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social). NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
Information Security Governance	The purpose of information security governance is to ensure that agencies are proactively implementing appropriate information security controls to support their mission in a cost-effective manner, while managing evolving information security risks. Information security governance has its own set of requirements, challenges, activities, and types of possible structures. Information security governance also has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities. NIST SP 800-100, *Information Security Handbook, A Guide for Managers, Chapter 2 Governance*
System Development Life Cycle	The system development life cycle (SDLC) is the overall process of developing, implementing, and retiring information systems. Various SDLC methodologies have been developed to guide the processes involved, and some methods work better than others for specific types of projects. Typically the following phases are addressed: initiation, acquisition, development, implementation, maintenance, and disposal. NIST SP 800-64 Rev. 1, *Security Considerations in the Information System Development Life Cycle*
Security Products and Services Acquisition	Information security services and products are essential elements of an organization's information security program. Agencies should use risk management processes when selecting security products and services.

Continued on next page

INFORMATION SECURITY PROGRAM ELEMENTS	
Security Products and Services Acquisition *(continued)*	As with the acquisition of products, the acquisition of services bears considerable risks that federal agencies must identify and mitigate. The importance of systematically managing the process for acquisition of information security services cannot be underestimated because of the potential impact associated with those risks. In selecting this type of services, agencies should employ risk management processes in the context of information technology security services life cycle, which provides an organizational framework for information security decision makers. NIST SP 800-35, *Guide to Information Technology Security Services*, provides assistance with the selection, implementation, and management of information security services by guiding the reader through the various phases of the information technology security services life cycle. Information security decision makers must consider the costs involved, the underlying security requirements, and the impact of their decisions on the organizational mission, operations, strategic functions, personnel, and service-provider arrangements. The process of selecting information security products and services involves numerous people throughout an organization. Each person involved in the process, whether on an individual or group level, should understand the importance of security in the organization's information infrastructure and the security impacts of their decisions. Depending on its needs, an organization may include all of the personnel listed below or a combination of particular positions relevant to information security needs. ◆ Chief Information Officer; ◆ Contracting Officer; ◆ Contracting Officer's Technical Representative; ◆ Information Technology (IT) Investment Review Board (IRB) or its equivalent; ◆ Security Program Manager; ◆ Information System Security Officer; ◆ Program Manager (Owner of Data)/Acquisition Initiator; and ◆ Privacy Officer. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services,* October 2003. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Technology Security Products,* October 2003.
Risk Management	The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Risk management can be viewed as an aggregation of three processes that have their roots in several federal laws, regulations, and guidelines. The three processes are risk assessment, risk mitigation, and evaluation and assessment. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
Certification, Accreditation, and Security Assessments	Security certification and accreditation (C&A) are important activities that support a risk management process, and each is an integral part of an agency's information security program. The C&A process is designed to ensure that an information system will operate with the appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically. Security controls are

Continued on next page

INFORMATION SECURITY PROGRAM ELEMENTS	
Certification, Accreditation, and Security Assessments *(continued)*	the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. **Security certification** is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **Security accreditation** is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. **Security Assessments** consist of two distinct tasks: 1) assessments conducted on an information system or a group of interconnected information systems and 2) completing an agency-wide security program-level questionnaire. To complete these tasks, an information security program must be established within the agency that supports the information system security life cycle. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
Configuration Management	Configuration management (CM) ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. CM should minimize the effects of changes or differences in configurations on an information system or network. The CM process reduces the risk that any changes made to a system (insertions/installations, deletions/uninstalling, and modifications) result in a compromise to system or data confidentiality, integrity or availability. An organization must ensure that management is aware of proposed changes and verify that a thorough review and approval process is in place. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Incident Response	A well-defined incident response capability helps an organization to detect incidents quickly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly. Federal civilian agencies are required to develop and implement procedures for detecting, reporting, and responding to security incidents. Agencies should also have a capability to provide help to users after a system security incident occurs and share information concerning common vulnerabilities and threats. NIST SP 800-61, *Computer Security Incident Handling Guide*
Contingency Planning	IT contingency planning is one element of a larger contingency and continuity of operations planning program that encompasses IT, business processes, risk management, financial management, crisis communications, safety and security of personnel and property, and continuity of government. NIST SP 800-34, *Contingency Planning for IT Systems*
Performance Measures	Performance measures are a key feedback mechanism for an effective information security program. Agencies can develop information security metrics that measure the effectiveness of their security program and provide data to be analyzed. NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*

WHAT ARE THE INFORMATION SECURITY LAWS, REGULATIONS, STANDARDS, AND GUIDANCE THAT I NEED TO UNDERSTAND TO BUILD AN EFFECTIVE SECURITY PROGRAM?

The United States Congress and OMB have instituted laws, regulations, and directives that govern creation and implementation of federal information security practices. These laws and regulations place responsibility and accountability for information security at all levels within federal agencies, from the agency head to system users. Furthermore, these laws and regulations provide an infrastructure for overseeing implementation of required practices, and charge NIST with developing and issuing standards, guidelines, and other publications to assist federal agencies in implementing the *Federal Information Security Management Act (FISMA) of 2002* and in managing cost-effective programs to protect their information and information systems. These laws, regulations, standards, and guidance—

- Establish agency-level responsibilities for information security;
- Define key information security roles and responsibilities;
- Establish a minimum set of controls in information security programs;
- Specify compliance reporting rules and procedures; and
- Provide other essential requirements and guidance

In addressing these requirements, agencies should tailor their information security practices to their organization's own missions, operations, and needs. The table below depicts the foundational information security laws, regulations, standards, and guidance that drive compliance and performance measurement for security programs. The table highlights three primary legislative sources for information security requirements. Following these, it presents additional sources that establish requirements for the overall agency management and influence agency implementation of information security requirements. The table also provides a brief description of the NIST standards and guidance that support these legislative requirements.

INFORMATION SECURITY LAWS, REGULATIONS, STANDARDS, AND GUIDANCE

Primary Sources	Overview
The Federal Information Security Management (FISMA) Act of 2002	Establishes the foundation of information security in the Federal government. As the primary legislation governing federal information security programs, FISMA builds upon earlier legislation through added emphasis on the management dimension of information security. FISMA delegates responsibility to develop detailed information security standards and guidelines for federal information systems, with the exception of national security systems, to NIST. ◆ FISMA designates OMB with the oversight of federal agencies' information security implementation.

Continued on next page

INFORMATION SECURITY LAWS, REGULATIONS, STANDARDS, AND GUIDANCE

Primary Sources	Overview
The Federal Information Security Management (FISMA) Act of 2002 *(continued)*	◆ FISMA provides a comprehensive framework for securing federal government information resources, including— ■ Defining key federal government and agency roles and responsibilities ■ Requiring agencies to integrate information security into their capital planning and enterprise architecture processes ■ Requiring agencies to conduct annual information security reviews of all programs and systems ■ Reporting the results of those reviews to OMB.
OMB Circular A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources*	Establishes a minimum set of security controls to be included in federal information security programs, assigns federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Homeland Security Presidential Directive 12 (HSPD-12)	This Presidential Directive was released in August 2004, and specifies a "policy for a common identification standard for all Federal employees and contractors."[1] HSPD-12 intends to increase identification security and interoperability by standardizing the process to issue a Federal employee or contractor an identification credential, and also by specifying the electronic and physical properties of the credential itself. The HSPD-12 credential is known as the Personal Identity Verification card.
Additional Sources	**Overview**
The Government Performance and Results Act (GPRA) of 1993	Establishes the foundation for budget decision making to achieve strategic goals in order to meet agency mission objectives. Establishes the requirement for federal agencies to develop, and submit to OMB and Congress, annual strategic plans. Each performance plan shall, among other things, briefly describe the operation processes, skills and technology, and the human capital, information, or other resources required to meet the performance goals. OMB issued Circular No A-130, Management of Federal Information Resources pursuant to this act.
The Paperwork Reduction Act (PRA) of 1995	Requires agencies to perform their information resource management activities in an efficient, effective, and economical manner. OMB issued Circular No A-130, Management of Federal Information Resources pursuant to this act. The term "information resources" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

[1] OMB, M-05-24, 'Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.'

INFORMATION SECURITY LAWS, REGULATIONS, STANDARDS, AND GUIDANCE	
Additional Sources	**Overview**
The Government Paperwork Elimination Act of 1998 (GPEA)	GPEA requires federal agencies to provide for the option of electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and use and acceptance of electronic signatures, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. To provide for a broad framework for ensuring the implementation of electronic systems in a secure manner, OMB directs agencies to use Circular A-130, Appendix III for guidance.
The Federal Financial Management Improvement Act (FFMIA) of 1996	FFMIA does three things: 1) Establishes in statute certain financial management system requirements; 2) Requires auditors to report on agency compliance with three stated requirements as part of financial statement audit reports; and 3) requires agency heads to determine, based on the audit report and other information, whether their financial systems comply with FFMIA. If not, agencies are required to develop remediation plans and file them with OMB. OMB implementation guidance for this act states that agencies shall ensure security over financial management information systems in accordance with OMB Circular A-130, Appendix 3. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data.
The Federal Managers Financial Integrity Act (FMFIA) of 1982	Requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency. This Act established the requirement for Executive agencies to have internal accounting and administrative controls in order to provide "reasonable assurance" that "funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation."
Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)	Supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources and: ◆ Focus on information resource planning to support their strategic missions; ◆ Implement a capital planning and investment control process that links to budget formulation and execution; and ◆ Rethink and restructure the way they do their work before investing in information systems.

INFORMATION SECURITY LAWS, REGULATIONS, STANDARDS, AND GUIDANCE	
Additional Sources	**Overview**
The E-Government Act of 2002	Promotes better use of the Internet and other information technology (IT) resources to improve government services for citizens and internal government operations and provide opportunities for citizen participation in government. The Act also requires agencies to— ◆ Comply with FISMA, included as Title III of the E-Government Act; ◆ Support government-wide, e-government initiatives; ◆ Leverage cross-agency opportunities to further e-government through the Federal Enterprise Architecture (FEA) initiative; and ◆ Conduct and submit to OMB privacy impact assessments for all new IT investments administering information in identifiable form collected from or about members of the public.
Standards and Guidance	**Overview**
NIST Federal Information Processing Standards (FIPS) csrc.nist.gov/publications/fips/index.html	FIPS are developed in accordance with the FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since the FISMA requires that federal agencies comply with these standards, agencies may not waive their use. See the following recent and relevant FIPS: ◆ FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* ◆ FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* ◆ FIPS PUB 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
NIST Special Publications 800 Series csrc.nist.gov/publications/nistpubs/index.html	Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. The special publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Office of Management and Budget policies (including OMB Memorandum, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST standards and guidance. Unlike FIPS which are compulsory and binding for federal agencies, SP 800 publications are not mandatory unless specified by OMB.
ITL Bulletins and NISTIRs csrc.nist.gov/publications/nistbul/index.html	Other security-related publications, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

WHERE CAN I LEARN MORE TO ASSIST ME IN EVALUATING THE EFFECTIVENESS OF MY INFORMATION SECURITY PROGRAM?

Several Federal government entities can be utilized to help an organization evaluate the effectiveness of their information security programs. Four key resources are listed below to assist with this evaluation.

Organization	Overview
National Institute of Standards and Technology www.nist.gov csrc.nist.gov	NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The Computer Security Division (CSD) is one of six divisions within NIST's Information Technology Laboratory. The mission of NIST's Computer Security Division is to improve information systems security by: ◆ Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies; ◆ Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems; ◆ Developing standards, metrics, tests and validation programs: ■ to promote, measure, and validate security in systems and services ■ to educate consumers and ■ to establish minimum security requirements for Federal systems ◆ Developing guidance to increase secure IT planning, implementation, management and operation.
Office of Management and Budget www.whitehouse.gov/omb	OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

Continued on next page

Organization	Overview
Office of Management and Budget *(continued)* www.whitehouse.gov/omb	In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public. Protecting the information and information systems on which the government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats. OMB has been designated to provide guidance to agencies through the requirements of the Federal Information Security Management Act of 2002. Under the act, OMB provides guidance for reporting weakness and corrective actions. The purpose of a Plan of Action and Milestones Report (POA&M) is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in **programs** and **systems**. In addition, OMB is evaluating agency information and information security in the President's Management Agenda Scorecard under the electronic government score. Agencies corrective action plans and quarterly updates on progress implementing their plans will be the basis for OMB's assessment of agencies' information system security for the Scorecard. This step will further reinforce the roles and responsibilities of agency program officials (bureau or division heads) for the security of systems that support their programs and the agency Chief Information Officer (CIO) for the agency-wide security program. It will also increase accountability and improve the security of the agency's operations and assets.
Government Accountability Office www.gao.gov	The Government Accountability Office (GAO) is an agency that works for Congress and the American people. Congress asks GAO to study the programs and expenditures of the federal government. GAO, commonly called the investigative arm of Congress or the congressional watchdog, is independent and nonpartisan. It studies how the federal government spends taxpayer dollars. GAO evaluates federal programs, audits federal expenditures, and issues legal opinions. When GAO reports its findings to Congress, it recommends actions. Its work leads to laws and acts that improve government operations, and save billions of dollars.
Federal CIO Council www.cio.gov	The Chief Information Officers (CIO) Council was established by Executive Order 13011, Federal Information Technology, on July 16, 1996. A charter for the Council was adopted on February 20, 1997, and later codified by the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The Council's role includes developing recommendations for information technology management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's information technology workforce. The Chair of the CIO Council is the Deputy Director for Management for the Office of Management and Budget (OMB) and the Vice Chair is elected by the CIO Council from its membership.

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti,
Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Content previously published in NISTIR 7359
January 2007

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930