# THE NEW FISMA STANDARDS AND GUIDELINES
## *CHANGING THE DYNAMIC OF INFORMATION SECURITY FOR THE FEDERAL GOVERNMENT*

Ron Ross, Stuart Katzke, and Patricia Toth
Computer Security Division
National Institute of Standards and Technology

## ABSTRACT

*The Federal Information Security Management Act (FISMA) of 2002 places significant requirements on federal agencies for the protection of information and information systems; and places significant requirements on the National Institute of Standards and Technology (NIST) to assist federal agencies to comply with FISMA. In response to this important legislation, NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project (http://csrc.nist.gov/sec-cert/index.html). This high-priority project includes the development of security categorization standards; standards and guidelines for the specification, selection, and testing of security controls for information systems; guidelines for the certification review and accreditation of information systems; and guidelines for the continuous monitoring of controls to ensure they continue to operate as intended. This paper includes a discussion of NIST's FISMA risk management framework (RMF) and the suite of related standards and guidelines being developed by NIST to help federal agencies comply with FISMA requirements (i.e., the FISMA suite of documents). In addition, the paper discusses how agency systems will benefit from applying the FISMA RMF, and why the FISMA RMF and the related suite of standards and guidelines should be of interest to other government sectors (e.g., DoD) and to the commercial sector.*

## INTRODUCTION

*The Federal Information Security Management Act (FISMA) of 2002* (http://csrc.nist.gov/policies/FISMA-final.pdf) places significant requirements on federal agencies for the protection of information and information systems; and places significant requirements on the National Institute of Standards and Technology (NIST) to assist the federal agencies comply with FISMA. In response to this important legislation, NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. This high-priority project includes the development of security categorization standards; standards and guidelines for the specification, selection, and testing of security controls for information systems; guidelines for the certification review and accreditation of information systems; and guidelines for the continuous monitoring of controls to ensure they continue to operate as intended.

The flagship standard among those developed by NIST is Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (http://csrc.nist.gov/publications/fips/index.html#fips199). This new mandatory standard, applicable to non-national security systems as defined by FISMA, will introduce some significant changes in how the United States Government protects its non-national security information and information systems including those government systems that comprise the nation's critical infrastructure.

The remainder of this paper discusses:

- FISMA's impact on federal agencies' IT security programs and on NIST's standards and research program;
- NIST's FISMA Implementation Project, including the FISMA risk management framework (RMF) and the project's suite of guidance and standards;
- The significant features of NIST's FISMA RMF;
- The benefits of the FISMA RMF to federal agency security programs; and
- The application of the FISMA RMF to commercial and other government sector information systems (e.g., DoD).

## FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 (TITLE III OF THE E-GOVERNMENT ACT)

***The E-Government Act of 2002 (Public Law 107-347,*** (http://csrc.nist.gov/policies/HR2458-final.pdf) recognizes the importance of information security to the economic and national security interests of the U.S. It promotes the development of electronic services and interagency collaboration to improve citizen access to information. The law aims to enhance access to information, while protecting personal privacy, national security, records retention, and access for persons with disabilities. The legislation establishes an Office of Electronic Government within the Office of Management and Budget (OMB) with an administrator who is appointed by the President. This office is responsible for coordinating and overseeing interagency collaboration, integrated projects, and improved access to government information and services. The Office of Electronic Government will manage an E-government fund to support innovative agency projects and a program to encourage contractors to develop innovative systems.

***Title III of the E-Government Act***, entitled the ***Federal Information Security Management Act (FISMA)***, addresses the need to enhance the effectiveness of information security controls of federal information systems. Among its many requirements, it requires each federal agency to develop, document, and implement an agency-wide program to improve the security of its information and information systems that support the operations and assets of the agency. The agency information security programs must include:

- **Periodic assessments of the risk and magnitude of the harm** that could result to the operations and assets of the agency;
- **Policies and procedures** that are based on risk assessments and cost-effective risk reduction;
- **Plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems;
- **Security awareness training** to inform personnel, contractors, and other users of agency information systems;
- **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, and practices, including the management, operational, and technical controls of every agency information system identified in their inventory;
- A process for planning, implementing, evaluating, and documenting **remedial action** to address any deficiencies;
- Procedures for detecting, reporting, and responding to **security incidents**; and
- Plans and procedures to ensure **continuity of operations** for information systems that support the operations and assets of the agency.

To support the federal agencies, FISMA tasks NIST to develop, among other things:

- **Standards to** be used by federal agencies to **categorize information and information systems** based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the **types of information and information systems to be included in each category**; and
- **Minimum information security requirements**, such as management, operational, and technical security controls, for information and information systems in each such category.

## NIST'S FISMA IMPLEMENTATION PROJECT

In response to FISMA, NIST initiated Phase I[1] of its FISMA Implementation Project. Phase I encompasses the risk management framework (RMF) of Figure 1. (described in more detail below). While the RMF is "system oriented" (i.e., focuses on protection of an information system and its related information), the overall context for the FISMA project is managing risks to the enterprise (e.g., federal agency, financial institution, power company, healthcare organization) that occur from breaches in security of its information systems and related information. Consequently, the RMF is much broader than the three tasks assigned to NIST under FISMA. In meeting its FISMA requirements, NIST also decided to take the opportunity to revise FIPS 102, its system security certification and accreditation guidance that was issued in 1983. The RMF also includes activities, such as risk assessment, security planning, and other security-related activities that occur within the system development life cycle.

[1] Phase II establishes a program to accredit organizations to perform security assessments in accordance with NIST Special Publications: 800-37, 800-53, and 800-53A.
Phase III (currently unfunded) establishes a program to validate vendor tools that claim to support the FISMA RMF.

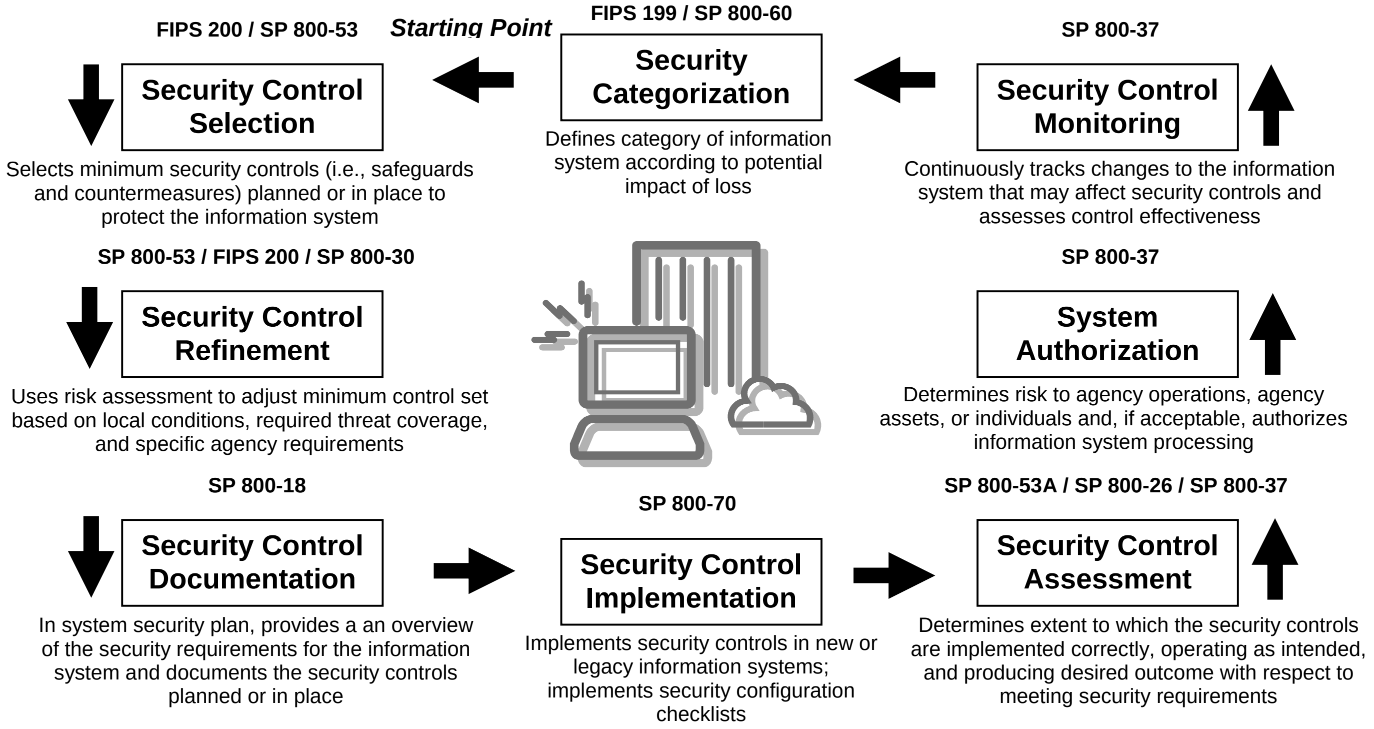
FIPS 200 / SP 800-53
Starting Point
FIPS 199 / SP 800-60
SP 800-37
Security Control Selection
Security Categorization
Security Control Monitoring
Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system
Defines category of information system according to potential impact of loss
Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness
SP 800-53 / FIPS 200 / SP 800-30
SP 800-37
Security Control Refinement
System Authorization
Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing
SP 800-18
SP 800-70
SP 800-53A / SP 800-26 / SP 800-37
Security Control Documentation
Security Control Implementation
Security Control Assessment
In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place
Implements security controls in new or legacy information systems; implements security configuration checklists
Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Figure 1. FISMA Risk Management Framework

Referring to Figure 1, we start a detailed description of NIST's FISMA Implementation Project with a discussion of FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199, effective February 2004, meets the FISMA requirement for NIST to develop "standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels." It is a mandatory federal standard that applies to all non-national security systems. It became effective on the day it was issued.

## FIPS 199

To gauge the importance and potential impact of FIPS 199 on the massive inventory of federal information systems, one must first understand how the world of information technology has changed over the past two decades. Not too many years ago, the information systems that populated federal enterprises consisted of large, expensive, standalone mainframes, taking up a significant amount of physical space in the facilities and consuming substantial portions of organizational budgets. Information systems during those times were viewed as "big ticket items" requiring specialized policies and procedures to effectively manage. Today, information systems are more powerful, less costly (for the equivalent computational capability), networked, and ubiquitous. The systems, in most cases, are viewed by agencies as commodity items—albeit items coupled more tightly than ever to the accomplishment of agency missions. However, as the technology raced ahead and brought a new generation of information systems into the federal government with new access methods and a growing community of users, some of the policies, procedures, and approaches employed to ensure the protection of those systems did not keep pace.

## THE PROBLEM WITH THE OLD WAY OF DOING BUSINESS

Abraham Lincoln once said, "You can fool some of the people all of the time and all of the people some of the time, but you cannot fool all of the people all of the time." The spirit of this quote can be applied appropriately to today's world of high technology in the methods used to protect agency information and information systems (including missions supported and services provided). The administrative and technological costs of offering a high degree of protection for all federal information systems at all times would be prohibitive, especially in times of tight governmental budgets. Achieving adequate, cost-effective information system security (as defined in Office of Management and Budget Circular A-130, Appendix III; http://www.whitehouse.gov/omb/circulars/a130/a130tran s4.html in an era where information technology is a commodity requires some fundamental changes in how the protection problem is addressed. This means that: ***Information systems must be assessed to establish priorities based on the importance of those systems to agency missions.***

There is clearly a criticality and sensitivity continuum with regard to agency information systems that affects the ultimate prioritization of those systems. At one end of the continuum, there are high-priority information systems performing very sensitive, mission-critical operations, perhaps as part of the critical information infrastructure. At the other end of the continuum, there are low-priority information systems performing routine agency operations. The application of safeguards and countermeasures (i.e., security controls) to all these information systems should be tailored to the individual systems based on established agency priorities (i.e., where the systems fall on the continuum of criticality/sensitivity with regard to supporting the agency's missions). The level of effort dedicated to testing and evaluating the security controls in federal information systems and the determination and acceptance of risk to the mission in operating those systems (i.e., security certification and accreditation) should also be based on the same agency priorities. Until recently, there were a limited number of standards and guidelines available to help agencies implement a more granular approach to establishing security priorities for their information systems. The result—many agencies would end up expending too many resources (both administratively and technologically) to protect information systems of lesser criticality/sensitivity and not enough resources to protect systems of greater criticality/sensitivity. Some "load balancing" was needed.

## USHERING IN A NEW ERA WITH FIPS 199 AND THE FISMA RMF

FIPS 199, the mandatory federal security categorization, provides the first step toward bringing some order and discipline to the challenge of protecting the large number of information systems supporting the operations and assets of the federal government. The standard is predicated on a simple and well-established concept—determining appropriate priorities for agency information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the system's criticality and sensitivity. FIPS 199 assigns this level of criticality and sensitivity based on the potential impact on agency operations (mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security due to the loss of confidentiality (i.e., unauthorized disclosure of information), integrity (i.e., unauthorized modification of information), or availability (i.e., denial of service). FIPS 199 requires federal agencies to do a "triage" on all of their information types and systems, categorizing each as low, moderate, or high impact for the three security objectives of confidentiality, integrity (including authenticity and non-repudiation), and availability.

Employed within a system development life cycle (SDLC), FIPS 199 and the FISMA RMF can be used as part of an agency's risk management program to help ensure that appropriate security controls are applied to each information system and that the controls are adequately assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The following activities, which are derived from the FISMA RMF in Figure 1., can be applied to both new and legacy information systems within the SDLC—

- ***Categorize*** the information system (and the information resident within that system) based on a FIPS 199 impact analysis (See **NIST Special Publication 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance in assigning security categories and refining the impact analysis.)
- ***Select*** an initial set of security controls for the information system (as a starting point) based on the FIPS 199 security categorization (See **NIST Special Publication 800-53**, *Recommended Security Controls for Federal Information Systems.*)[2]
- ***Refine*** the initial set of security controls selected for the information system based on local conditions including agency-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or other special circumstances. (See **NIST Special Publication 800-30**, *Risk Management Guide for Information Technology Systems.*)
- ***Document*** the agreed-upon set of security controls in the system security plan including the agency's rationale and justification for any refinements or

[2] **FIPS 200**, *Security Controls for Federal Information Systems*, will replace NIST Special Publication 800-53 in December 2005 in fulfillment of the FISMA legislative requirement for mandatory minimum security requirements for federal information systems.

adjustments to the initial set of controls (See NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*)

- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place. (See NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle.*)
- ***Assess*** the security controls using appropriate methods and procedures 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. (See NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* initial public draft projected for publication spring 2005.)[3]
- ***Determine*** the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the planned or continued operation of the information system (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*)
- ***Authorize*** system processing (or for legacy systems, authorize continued system processing) if the level of risk to the agency's operations, assets, or individuals is acceptable to the authorizing official (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*)
- ***Monitor*** selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate agency officials on a regular basis (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*).
- ***Significant changes*** to the information system or the security requirements for that system may prompt the agency to revisit the above activities.[4]

## SIGNIFICANT FEATURES OF THE RMF

The FISMA RMF and associated suite of standards and guidelines contains features that enable more cost-effective utilization of IT security resources. These include:

- A standard security categorization method for an information system that applies to all federal non-national security information and information systems (FIPS 199). It is based on a worst-case impact assessment to the enterprise if there is a compromise in confidentiality, integrity, and/or availability of the information in an information system and to the system itself.
- The security categorization standard supports prioritization of an enterprise's systems, allowing enterprises to apply security effort to the highest impact systems first.
- The security categorization standard supports scaling of the level of security effort, allowing enterprises to apply security effort commensurate with the security categorization of their information systems.
- A master control catalogue that contains a basic versions of each control in the catalogue with (possibly) one or more enhancements (SP 800-53).
- A set of minimum baseline controls for Low, Medium, and High impact systems that have been preselected_by NIST from the control catalogue. (NIST SP 800-53). The baselines are hierarchical since the controls in each baseline increase in functional and assurance requirements and contain all of the controls of the lower baseline.
- The concept of common security controls and the reusability of security assessment results of the common security controls. The reuse of security assessments of common controls can reduce the control assessment effort required in assessing the information system's controls that use/depend on the common control sets. Common information system security-related controls include:
  - Agency-wide controls (e.g., training, personal security)
  - Site-wide controls (e.g., physical security, contingency plan)
  - Common subsystem controls (e.g., a common software package deployed at multiple sites)
- The concept of certification and accreditation (C&A) for low impact systems that allows for a scaled level

[3] The determination of security control effectiveness during the assessment process may require remedial actions such as employing additional controls or fixing controls that are ineffective. See NIST Special Publication 800-53.

[4] A significant change is typically defined as any change to the hardware, software, or firmware components of an information system that may have an impact on the protection capabilities of that system and the enforcement of the system security policy. Examples include such things as the installation of a new or upgraded operating system, firewall, database management system, network device, or identification and authentication mechanism.

of effort (e.g., a self-assessment process) to significantly reduce the level of effort of C&A for such systems.

- Assurance requirements that are baseline-dependent (i.e., the same for each control in a particular minimum control baseline). As the baselines increase, there is a corresponding increase required in the control developer/implementer's analysis and evidence to demonstrate implementation quality, correctness, and confidence.
- Assurance requirements are related to and support the control assessment approach in NIST SP 800-53A.

## THE BENEFITS OF THE FISMA RMF TO AGENCY SECURITY PROGRAMS

The long-term effect of employing the FISMA RMF approach to federal agencies' information systems is better, more targeted, and cost-effective security for these systems. While the interconnection of information systems often increases the risk to an agency's operations and assets, the FISMA RMF provides a common approach and understanding for expressing information security, and thus promotes greater consistency across diverse enterprises in managing that risk. Agencies will determine which information systems are the most important to accomplishing assigned missions based on the security categorization of those systems and will protect the systems appropriately. Agencies will also determine which systems are the least important to their missions and will not allocate excessive resources for the protection of those systems.

In the current high technology era where information systems are viewed as commodities and are routinely used to protect some of the nation's most important assets within the ~~F~~ government and the critical infrastructure, the FISMA RMF is right for the time. In the end, the new FISMA RMF suite of security standards and guidelines, when properly applied, will facilitate a more effective allocation of available resources for protecting information systems, determine the need and provide a justification for the allocation of additional resources, and result in a substantial improvement in the security posture of the government's information systems.[5]

## APPLICATION OF FISMA RMF IMPLEMENTATION GUIDANCE SUITE TO COMMERCIAL SECTOR SECURITY PROGRAMS

While NIST guidance is intended for federal agencies, the FISMA RMF (including the associated suite of standards and guidance documents) is not government centric—it applies equally well to commercial enterprises~~,~~ as to federal agencies. While there is no requirement that commercial sector enterprises use the approach discussed in this paper, it is possible that the mandatory use of FIPS 199 by federal agencies will cause FIPS 199, the FISMA RMF, and the associated suite of documents to become standards of "due diligence" within the federal community. Given the connections between the private and government critical infrastructure sectors through sector liaisons, it is possible that the same level of due diligence will be expected of the private sector critical infrastructures. Consequently, there may be suggestions from the government that the government would like to see at least as robust approach in protecting private critical infrastructure systems as those discussed here for non-national security federal systems.

In addition, there are other compelling reasons why the commercial sector should consider adopting or adapting this approach. These include:

- NIST has contributed the FISMA RMF and the associated document suite to an IEEE Information Assurance standards working group as candidates for common industry-government standards (http://issaa.org/). The IEEE standard is called, "The Information System Security Assurance Architecture (ISSAA)." The ISSAA is IEEE's version of the FISMA RMF. Although NIST's FISMA suite of documents will be contributed to the IEEE working group (WG) as candidates for individual IEEE standards (as part of the overall ISSAA effort), the WG has the option to adopt or adapt NIST's documents or to develop their its own preferred approach (as long as it is consistent with the intent of the ISSAA/FISMA RMF).
- The control catalogue and the minimum control sets/baselines (found in NIST SP 800-53) incorporate security controls from and are consistent with many public and private sector sources of controls such as: Common Criteria Part 2, ISO/IEC 17799, COBIT, GAO FISCAM, NIST SP 800-26 Self-Assessment Questionnaire, CMS (healthcare),

[5] The FISMA-related security standards and guidelines discussed in this article are available at the FISMA Implementation Project web site at http://csrc.nist.gov/sec-cert.

D/CID 6-3 Requirements, DoD Policy 8500, and BITS functional packages.[6]

- Controls can be added to the control catalogue and new control baselines developed to meet the requirements of community-specific information technology (IT) applications/systems. Examples include commercial sector communities that need to meet the security requirements of SCADA/real-time processing systems, healthcare/—HIPAA, and financial/Sarbanes-Oxley.
- Commercial sector organizations that operate information systems on behalf of the government (e.g., contractors, IT service providers, IT outsourced services) are required to meet FISMA requirements. It is likely that such organizations will find it easier to implement and provide the same set of controls (at least) for their commercial customers as they do for their government customers.
- In Phase II of the FISMA Implementation Project, NIST plans to work with professional and academic organizations to establish an accreditation program for accrediting organizations that are competent to perform the security controls assessments process specified in SP 800-53. The goal of this activity would be to establish a source/pool of competent security controls assessment organizations that could be hired by government agencies to assist with their security assessments. It is anticipated that if NIST establishes the accreditation program through an open public process in partnership with credible professional or academic organizations, private sector enterprises would prefer to utilize the same source for their controls assessment tasks. So, for example, we envision that cyber insurance companies might use these accredited professionals to assess the security controls of a potential client prior to issuing the client a cyber insurance policy.
- All NIST standards and guidelines go through an open public review process, often including one or more public workshops. During a typical review process, NIST receives numerous comments/suggestions from both government and commercial sector organizations—and takes these into consideration as it develops the next drafts of the documents. In particular, NIST invites industry review and comment on the applicability of NIST standards/guidelines to commercial sector systems since, in many cases, government and industry have the same requirements. When this coordination is done properly, we find that commercial sector organizations heavily utilize NIST guidance.

## CONCLUSION

The FIPS 199, the FISMA RMF, and the associated suite of guidance documents will significantly change the processes federal agencies use to categorize and prioritize their systems; select, document, and implement system security controls; perform certifications and accreditations, and perform continuous monitoring of controls to ensure they continue to operate as intended—resulting in more cost-effective, uniform, consistent, and improved information systems security and overall reduced risk to the agencies. We also believe that the approach discussed here is appropriate for commercial sector use—and encourage commercial sector enterprises to use them. We invite an open public dialogue on this approach and on the applicability of the approach to the private sector.

[6] COBIT stands for Control Objectives for Information and related Technology and is an open standard for control over information technology, developed and promoted by the IT Governance Institute, http://www.itgi.org/. Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM) http://www.gao.gov/special.pubs/afm.html AIMD-12.19.6, June 2001. Revised NIST Special Publication 800-26 System Questionnaire with NIST SP800-53 References and Associated Security Control Mappings, April 2005 at http://csrc.nist.gov/publications/nistpubs/index.html. Centers for Medicare & Medicaid Services (CMS) is a Federal agency within the U.S. Department of Health and Human Services, http://www.cms.hhs.gov/. BITS is a nonprofit CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the U.S., http://www.bitsinfo.org/.