NIST DELIVERS STRONG AND FLEXIBLE SECURITY STANDARDS

Managing Enterprise Risk in a World of Sophisticated Cyber Threats

Dr. Ron Ross
National Institute of Standards and Technology

Today's information systems face increasingly sophisticated cyber threats. The risks to critical missions and business functions being carried out by federal agencies and their support contractors is of growing concern to the United States Congress and the Office of Management and Budget. Recent federal legislation enacted after the September 11, 2001, terrorist attacks, described the increasing dependence on information technology and the protection of enterprise missions as a problem of national and economic security that encompasses both government and industry.[1] The nation's critical infrastructure[2] must be protected. Yet our critical infrastructure is fragile as illustrated by the great blackout of 2003 which left over 50 million people without electricity for an extended period of time after a series of cascading power plant failures across the northeastern United States and Canada. Since the critical infrastructure within the United States is over ninety percent owned and operated by nonfederal entities (including state, local, and tribal governments, private sector firms, and commercial industry), any potential solutions addressing the difficult and challenging protection problems must be broad-based and resonate with both the public and private sectors.

A Call to Action—Strengthening the Information Technology Infrastructure

Congress, recognizing the increasing reliance on information technology and the growing risks to the nation based on an ever-expanding threat base and growing sophistication of cyber adversaries, passed the Federal Information Security Management Act (FISMA) of 2002.[3] The FISMA legislation established broad and sweeping information security requirements for the federal government. The National Institute of Standards and Technology (NIST) retained specific responsibilities under the Act to develop a full range of implementing security standards and guidelines that would enable federal agencies to comply with the legislation. NIST had the challenging task of establishing mandatory minimum security standards and guidelines for the federal government and private sector support contractors (also covered by the legislation) while ensuring sufficient flexibility in the implementation of those standards and guidelines based on a very diverse set of federal missions and business functions and an equally diverse set of federal agencies carrying out those missions and business functions.

Establishing a Unified Framework for Managing Enterprise Risk

To meet the challenge of establishing mandatory minimum information security standards and guidelines and maintaining the needed flexibility of application and implementation, NIST first developed a generalized framework for managing enterprise risk with regard to information systems that support organizational missions and business functions. The Risk Management Framework (RMF), illustrated in Figure 1, provides a comprehensive vehicle for federal agencies to use in building information security into the infrastructure of the organization. The RMF

[1] USA PATRIOT Act (Public Law 107-56), October 2001.

[2] The U.S. critical infrastructure includes the energy sector (electrical, nuclear, gas and oil, dams), transportation sector (air, road, rail, port, waterways), public health and emergency services sector, information and telecommunications sector, national defense sector, banking and finance sector, postal and shipping sector, agriculture, food, and water sector, and chemical sector.

[3] The Federal Information Security Management Act (FISMA) is part of the E-Government Act of 2002 (also known as Public Law 107-347).

promotes a disciplined, structured, and flexible process for applying the NIST security standards and guidelines[4] based on specific missions, business functions, operational environments, technologies, and threat conditions. The RMF represents the security-related activities which occur within an enterprise's System Development Life Cycle (SDLC) and can be adapted by private sector organizations that are not covered under the FISMA legislation using the "plug and play" features of the framework which allow the use of any security categorization approach, risk assessment, set of security controls, or assessment process. NIST continues to strive for broad-based, consensus standards by working with the IEEE[5] to move the RMF into the national and international standards community.

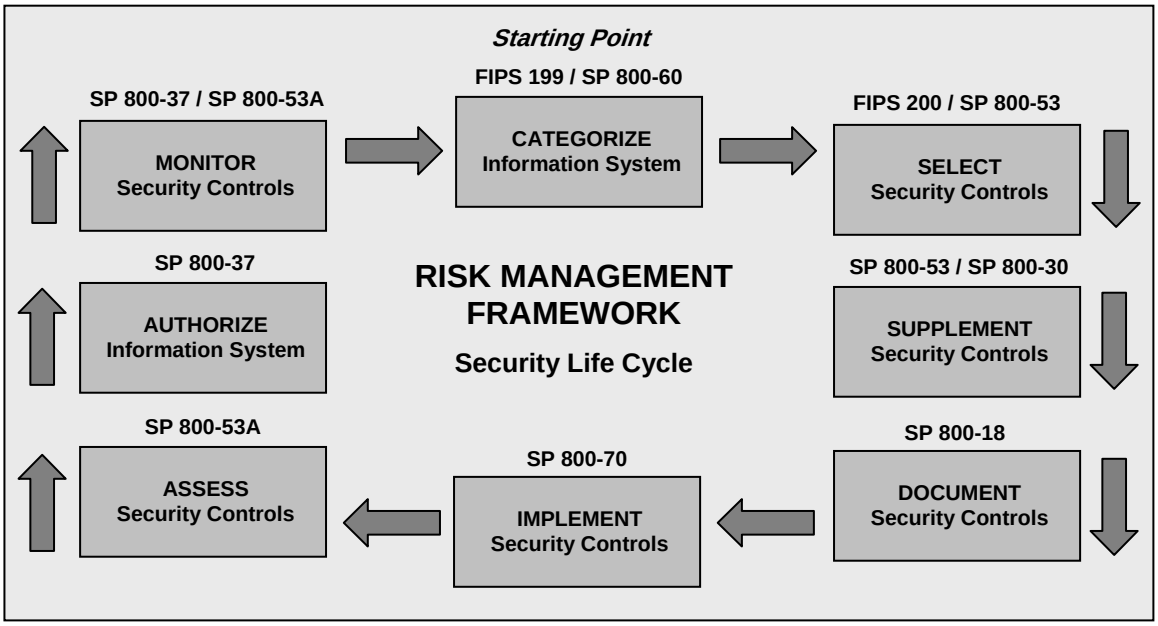

FIGURE 1: THE RISK MANAGEMENT FRAMEWORK

NIST FISMA standards and guidelines rest on a solid foundation of core principles with regard to the protection of federal information systems and the information processed, stored, and transmitted by those systems. The core principles and the linkage to the RMF and NIST security standards and guidelines are described in the following sections.

Identifying and Prioritizing Information System Assets Requiring Protection

Establishing a well-defined information system boundary and understanding the mission or business case impact resulting from a breach or compromise to the confidentiality, integrity, or availability of the system is the first step an organization takes in building an effective information security program. FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems*, the first FISMA-related mandatory standard required by Congress, provides a straightforward and simple impact categorization approach. FIPS 199 is a worst-case assessment of mission or business case impact should the core information technology capability of an enterprise be compromised by a cyber attack. The worst-case analysis is used

[4] The current NIST FISMA-related security standards and guidelines associated with each step in the Risk Management Framework are listed in Figure 1. Security standards are denoted as Federal Information Processing Standards (FIPS) and security guidelines are denoted as Special Publications (SP). These standards and guidelines can be found at http://csrc.nist.gov.

[5] IEEE P1700, Standard for Information System Security Assurance Architecture (ISSAA).

due to the inherent difficulty in predicting with any degree of confidence, the probabilities of the multitude of threat exploitations of information system vulnerabilities and the corresponding impacts that could result. In essence, in today's world of complex information technologies, ubiquitous networks, and worldwide connectivity, all threats must be considered during the initial planning phases of the enterprise protection strategy. The prioritization of information technology assets under FIPS 199 also recognizes that an enterprise cannot afford to protect all of its information system assets and operations to the highest levels at all times. The FIPS 199 security categorization drives the rigor, intensity, and level of effort applied by the organization to each activity within the RMF—that is, providing the starting point for applying the needed flexibility to allocate security resources in a scalable manner based on the criticality and/or sensitivity of the enterprise mission or business functions.

Selecting Minimum Baseline Security Controls and Tailoring the Baseline

Since the security categorization process considers worst-case mission or business case impacts due to breaches in the information system and the potential loss or compromise in the confidentiality, integrity, or availability of enterprise information, the high water mark[6] approach is employed to select an initial set of security controls as a starting point. The high water mark, while initially appearing to over specify the security control requirements for the information system, is only a transitory step in the overall control selection process. NIST Special Publication 800-53 provides both an initial set of security controls for federal information systems and also extensive tailoring guidance for agencies to use in achieving the needed flexibility in adjusting the controls to cost-effectively meet mission and business case requirements. The flexibility built into the security standards and guidelines is extensive, including: (i) techniques for scoping the controls to meet operational requirements, environmental conditions, and technology availability; (ii) approaches for applying compensating controls when necessary; and (iii) methods for applying specific parameters to the controls to reflect the specific requirements of the agency implementing the controls. At the end of the tailoring process, agencies can have a "customized" set of security controls that are documented in their information system security plans—again, based on strong, but flexible security standards and guidelines suitable to the task. The aggressive use of tailoring guidance ensures that the NIST security standards and guidelines are applied in a "common sense" manner—ensuring that only necessary security controls are included.

Supplementing the Minimum Security Controls Based on Organizational Assessments of Risk

Given the sophistication of today's cyber threats and the rich targets of opportunity provided by federal information systems, it is imperative that the NIST security standards and guidelines not only be flexible in nature but also extensible. In that light, risk assessment still plays an important part in the agency's information security program and overall protection strategy. Once the baseline security controls have been selected and tailored based on the initial FIPS 199 impact, agencies must continue the process of carrying out their security due diligence by selecting additional security controls to supplement the tailored baseline controls based on an organizational assessment of risk. The risk assessment is employed in a more targeted manner to consider additional threat information, specific mission requirements, operating environments, and any other factors that may affect the successful accomplishment of the agency's mission or

[6] The high water mark concept is employed in NIST Special Publication 800-53 because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective; rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level.

business functions. Appropriate security controls or security control enhancements can be added to the system security plan from the NIST Special Publication 800-53 catalog, demonstrating the organization's commitment to increasing the level of security in the information system beyond the required minimum baselines. Once agencies have an agreed-upon set of security controls, those controls are documented in the security plans for the information systems and subsequently implemented. It is important to note that the resulting set of security controls has been determined by the organization, not by NIST. The NIST guidance provides common starting points based upon FIPS 199 categorization, a catalog of security controls from which to select, and a common process for arriving at the necessary and sufficient set of controls for an information system. A key element of the NIST approach is to empower the enterprise with needed flexibility by providing "ownership" of the resulting risks to the organization's operations and assets, individuals, other organizations,[7] and the nation.

Assessing Security Control Effectiveness and Determining Acceptable Levels of Risk

Employing a strong set of security controls to protect enterprise missions and business functions is a top priority for organizations in today's highly networked operating environments. Knowing if the security controls selected and implemented are effective in their application is equally important. Most information systems have thousands of flaws, some inherent in the commercial information technology products that are a part of the system and some inherent in the manner in which the systems are put together. When information system flaws can be exploited by threat sources, the flaws become vulnerabilities. Security controls are employed by organizations to counter information system vulnerabilities; the fewer vulnerabilities remaining in the system, the smaller the target of opportunity for threat sources intent on exploiting those vulnerabilities. The senior leadership within the agency must decide if the remaining vulnerabilities in the information system after the employment of agreed-upon security controls are significant enough to place the agency's mission or business functions at an unacceptable level of risk. Determining the effectiveness of the management, operational, and technical security controls supporting the information system through a structured and disciplined assessment process provides the necessary information to organizational officials to make credible decisions on accepting risk to the organization's operations and assets, individuals, other organizations, and the nation. It is critical to have the appropriate visibility into the true security state of the information system in order to make such important decisions for the agency. NIST security standards and guidelines provide a comprehensive approach for making these risk-based determinations and, at the same time, incorporate the needed flexibility to ensure cost-effective implementations[8] of the assessment process.

Continuous Monitoring—Ongoing Visibility into the Security State of the Information System

Continuous monitoring of an information system's security controls is becoming increasingly important due the dynamic nature of the current environments in which federal agencies and their support contractors operate. Changes to hardware, software, environments of operation, missions, implementing technologies, and people have the potential to perturb the security state

[7] The risk to "other organizations" occurs through partnering relationships in which one organization shares information with another organization and the other organization depends on the confidentiality, integrity, or the availability of that information.

[8] In support of the FISMA Implementation Project, NIST has initiated the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) that promotes effective, efficient, and consistent security assessments. SCAP facilitates the automated application, verification, and reporting of commercial information technology product-specific security configuration settings, thereby reducing vulnerabilities when products are not configured properly. Information on the ISAP/SCAP initiative can be found at http://nvd.nist.gov.

of the information system at any time. NIST security standards and guidelines describe a flexible and dynamic approach for monitoring the security status of agency information systems. Strong configuration management and control processes for information technology assets, security impact analyses of changes to the information system, and a reasoned strategy for assessing selected subsets of security controls on an ongoing basis, form the core of the continuous monitoring process described in the NIST publications. A well thought out enterprise-wide continuous monitoring program ensures that agency officials will continue to receive the information necessary to determine the true security state of their information systems and if the resulting level of risk to the organization's operations and assets, individuals, other organizations, and the nation continues to be acceptable.

Focusing on the Enterprise—The Corporate View of Information Security

Information systems do not exist in isolation within enterprises today. The information systems are, in most cases, the engines that enable organizations to be productive and successfully conduct important organizational missions, for example, controlling electric and water distribution systems, issuing pay checks, monitoring patient's conditions in hospitals, and providing business communications. Information security programs must be applied at the enterprise-wide level considering the contributions of all information systems to supporting the critical missions and business functions of the organization. NIST security standards and guidelines recognize the enterprise-wide view of security and have incorporated effective techniques to address information security issues both at the information system level and at the enterprise level. For example, NIST Special Publications identify a type of security control known as a "common control" which is a safeguard that is developed, implemented, and assessed at the enterprise level of an organization and supports multiple information systems. These "infrastructure-based" security controls, if developed as an enterprise-wide exercise with the involvement of the senior leadership, have the potential to produce significant cost savings for organizations and more consistent information security across the enterprise as a whole. NIST security standards and guidelines support a bottom-up approach to security focusing on the individual information systems supporting the enterprise, and a top-down approach to security focusing on specific information security-related issues from the corporate perspective—thus, facilitating significant enterprise-wide cost savings and efficiencies.

Development Paradigm for NIST Security Standards and Guidelines

NIST security standards and guidelines are developed through an open, public vetting process that involves a significant level of review and comment from both public and private sector entities. The key FISMA-related security standards and guidelines developed by NIST as part of the FISMA Implementation Project, to include FIPS 199, FIPS 200, and NIST Special Publications 800-37, 800-59, 800-60, 800-53, and 800-53A, have gone though an intensive public vetting process with thousands of inputs received from a very broad base of customers (both individuals and organizations) that will be using the standards and guidelines either on a compulsory or voluntary basis. The purpose of the comprehensive vetting process is to ensure that the NIST security standards and guidelines are technically sound, cost-effective, state-of-the-practice, and able to be implemented by organizations affected by the FISMA legislation. To facilitate timely updates to the security standards and guidelines based on changing threats, vulnerabilities, and information technologies, NIST commits to regular and ongoing modifications of its publications. Updates to publications go through the same rigorous public vetting process, maximizing input from customers in the public and private sectors.

Growing Use and Acceptance of NIST Security Standards and Guidelines

The use of NIST security standards and guidelines is mandatory for federal agencies and contractors operating information systems on behalf of federal agencies. State, local, and tribal governments, as well as private sector organizations are encouraged to use the standards and guidelines on a voluntary basis. There is evidence of growing use and acceptance of the NIST security standards and guidelines in important communities of interest such as the national security community, healthcare industry, and financial services sector. For example, the Office of the Director of National Intelligence (DNI) and the Department of Defense (DoD) are collaborating on a joint initiative that will institute sweeping reforms of the security policies, practices, and certification and accreditation process for the Intelligence Community and the Unites States military. The changes in the DNI and DoD information security policies, practices, and processes will be largely based on the foundation established by the current NIST security standards and guidelines including FIPS 199, Special Publication 800-53, and the Risk Management Framework. Private sector organizations are also demonstrating an uptake in the use of NIST security standards and guidelines, not due to FISMA requirements, but because strong management, operational, and technical safeguards for corporate information systems help secure critical business functions and promote customer confidence in the ability of corporations to protect personal information.

The Transition to a More Secure Information Technology Infrastructure

The transition to full implementation of NIST's FISMA-related security standards and guidelines continues at a rapid pace. NIST has attempted to balance the Congressionally mandated requirements in the FISMA legislation with the realities and needs of a large and diverse federal government and supporting information technology infrastructure conducting critical operations and providing services to citizens on an ongoing basis. The size and complexity of the undertaking continues to be one of the greatest challenges for the federal government. The flexibility of NIST's security standards and guidelines gives federal agencies and their support contractors the appropriate tools to demonstrate compliance to the FISMA legislation. Compliance is not just a paperwork drill—it is exercising the security due diligence that protects critical enterprise operations and assets, individuals, other organizations, and the nation. The stakes have never been higher, and failure is not an option.