Global Information Assurance Certification Paper

Lincoln Warren
GSEC Practical Assignment v. 1.4 (Option 1)

"FISMA and the NIST Security Certification and Accreditation Project."

Abstract

On December 17th, 2002, "The E-Government Act of 2002" (H.R. 2458) was passed into law. Title III of this law is known as the "Federal Information Security Management Act of 2002" (hereby referred to as FISMA). FISMA will require every federal agency develop and maintain an information security program, and to have its information systems reviewed and accredited on the basis of security. The categories of information systems, the standards for accreditation, and the processes for accreditation and certification of systems are to be developed by the National Institute of Standards and Technology (hereby referred to as NIST).

This paper will briefly discuss some of the legislation cooperating with and leading up to FISMA. It shall then discuss in detail the requirements of FISMA. Next, the work of NIST shall be investigated. Specifically, NIST is in the process of writing a set of documents that will set the guidelines and standards for the accreditation and certification of information systems. This undertaking is called the Security Certification and Accreditation Project. The phases of this project will be discussed in detail.

In conclusion, a summary of the certification and accreditation process is given. The significance of this legislation, and the work of the NIST, to the information security community will be discussed.

Background

"The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States." (Circular No. A-130)

If this is true, than we would certainly expect the Federal Government to take the lead in developing information security policy. Indeed, the feds have passed numerous pieces of documentation and legislation that have recognized the importance of computer security.

Let's start our timeline on December 30th, 1985. On this day, "Appendix III of the Office of Management and Budget (OMB) Circular No. A-130" defined a minimum set of controls for the security of federal automated information systems. This document (also known as "Security of Federal Automated Information Systems) defined controls for federal information systems that were considered effective in centralized computing environments. These

environments generally ran custom-developed software. While an important step at the time, it would not be long before vast and comprehensive changes in computing would develop, and guidelines would have to adapt.

The Computer Security Act of 1987 was passed into public law on January 8, 1988. This act recognized that providing security for public systems was "in the public interest," and assigned the task of developing standards and guidelines for computer security to the National Bureau of Standards (now known as the NIST). It also established the Computer System Security and Privacy Advisory Board. This board, which operates under the Department of Commerce, was tasked to "identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy." This act showed that the government recognized computing environments were becoming more open and widely distributed. Commercial software was also becoming more common. It is important to note that Circular No. A-130 was revised as a result of this legislation.

In 1995, the Paperwork Reduction Act was signed into law. This act was significant because it requires agencies to establish computer security programs, and gives the OMB the task of developing, overseeing, and implementing policies and guidelines on information security. Circular No. A-130 was given its latest revision to reflect these new responsibilities.

In 1996, "The Information Technology Management and Reform Act of 1996" (also known as the Clinger-Cohen Act) was passed into law. Section 5131 of this act is called "Responsibilities Regarding Efficiency, Security, and Privacy of Federal Computer Systems." This section gives the Secretary of Commerce the authority to make the information security standards of the NIST compulsory and binding "to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems." This is significant because it gives power of enforcement that had been lacking in other documents.

Perhaps the most significant legislation related to information security; however, was passed and signed into law in December of 2002. Title III of the E-Government Act, titled the "Federal information Security Management Act" (FISMA), requires every federal agency to develop, *document,* and *implement* an agency-wide information security program. This act, combined with the Paperwork Reduction Act of 1995 and Clinger-Cohen, turn the guidelines developed by the NIST into mandates.

FISMA

The E-Government Act defines Electronic Government as the government use of "web-based Internet applications or other information technology to enhance the access to and delivery of government information and services to the public,

other agencies, and other government entities; or to bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation." The Act establishes a new agency under the OMB called the Office of Electronic Government. This office is responsible for promoting cooperation in information management so as to improve public services. The new agency will also oversee the E-Government Fund, which was established to fund projects that will allow the public easier access to information and government services. This important step in establishing the importance of information *technology* in government also increases the importance of information *security* in government. One of the purposes of FISMA, as stated in section 3541, is "to provide for development and maintenance of minimum controls required to protect Federal information and information systems." Another is to "provide a mechanism for improved oversight of Federal agency information security programs." These information security programs are not only to be developed and implemented, but will also be reviewed "at least" annually. If the NIST guidelines are not met, these systems will be taken offline.

The development of these guidelines and standards are a huge responsibility, and will surely affect the entire Information Security community. This task has been given to NIST. They have undertaken this task by forming the Security Certification and Accreditation Project (hereby referred to as SCAP).

NIST and the Security Certification and Accreditation Project.

According to the Initial Public Draft of FIPS Publication 199, FISMA has tasked 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;
- Guidelines recommending the types of information and information systems to be included in each category, and
- Minimum information security requirements, (i.e., management, operational, and technical security controls), for information and information systems in each category.

To accomplish these tasks, NIST launched the Security Certification and Accreditation Project. According to the project website, the vision for this project is to:

Promote the development of-

- Guidelines for certifying and accrediting federal information systems including the critical infrastructure of the United States;

- Security controls for information systems supporting the security objectives of confidentiality, integrity, and availability;

- Techniques and procedures for verifying the effectiveness of security controls applied to federal information systems;

- Robust, automated tools supporting the security certification and accreditation process; and

- Public and private sector assessment organizations capable of providing cost effective, high quality, security certification services.

Leading to-

- More consistent, comparable, and repeatable evaluations of security controls applied to federal information systems;

- A better understanding of agency-related risks resulting from the operation of information systems;

- More complete, reliable, and trustworthy information for authorizing officials---thus, facilitating more informed security accreditation decisions; and

- More secure information systems within the federal government.

This project will be accomplished in two phases. Phase One is to develop standardized guidelines for conducting security certifications and accreditations of federal information systems. Phase Two is to create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the standardized guidelines that have/will be laid out in Phase One.

Before we discuss the two phases, there is one important document the NIST has released that lays the foundation for SCAP: FIPS Publication 199.

FIPS Publication 199

The Computer Security Act of 1987 states that the information security policy of a federal system must be "commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. " This has held throughout all legislation relating to the security of federal information. One of

the tasks given to NIST was to develop concrete standards for categorizing information and information systems based on risk. FIPS Publication 199 is the document that addresses this task.

According to FIPS Pub. 199, risk is determined by assessing the *threat* of an attack that would lead to loss of confidentiality, integrity, or availability of an information system, and the *impact* or magnitude of harm to agency operations that would occur from the loss of confidentiality, integrity or availability of these systems. Though threat and impact are both considered, impact is generally given more weight in determining the risk factor.

FISMA gives the following definitions:

- **Confidentiality**: "Preserving authorized restrictions of information access and disclosure, including means for protecting personal privacy and proprietary information…"
- **Integrity**: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"
- **Availability**: "Ensuring timely and reliable access to and use of information…"

A loss of confidentiality would be the unauthorized *disclosure* of information. A loss of integrity would be the unauthorized *modification* of information. A loss of availability would be the disruption of *access* to information. The categorization of information is based on the risk-level of each of these three security objectives.

RISK-LEVEL = [THREAT + IMPACT) (more weight given to impact)
CATEGORY = [(Confidentiality, risk-level) + (Integrity, risk-level) + (Availability, risk-level)]

FIPS Publication 199 defines three levels of risk: **low, moderate, and high.** A low risk system would be a system that losses of confidentiality, integrity, and availability would have "limited adverse on agency operations…assets, or individuals." A moderate risk system would be a system that losses of confidentiality, integrity, and availability would cause "significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets." A high-risk system would be a system where losses of confidentiality, integrity, and availability would have "a severe or catastrophic adverse effect on agency operations…assets, or individuals." This would include a "loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets." The level of security controls given to an information system should be based on its risk level.

Phase One

Phase One of SCAP involves NIST releasing a series of three documents that together will provide a comprehensive solution to categorizing and protecting federal information systems. One of these documents has been released, and the other two will be released within the year. The list of "Phase One" documents is as follows:

- NIST Special Publication 800-37 "Guide for the Security Certification And Accreditation of Federal Information Systems" (Initial public draft) Released in June 2003.
- NIST Special Publication 800-53 "Guide for the Selection and Specification of Security Controls for Federal Information Systems" (Initial public draft projected to be published Summer 2003)
- NIST Special Publication 800-53A "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems" (Initial public draft projected for publication, Winter 2003-04)

NIST Special Publication 800-37

This document, "Guide for Security Certification and Accreditation of Federal Information Systems", was released as a second public draft in June of 2003. (Note: The first public draft was released in 2002. The passing of FISMA required significant updates to the document, which are reflected in the new version). This important document was written to define guidelines for the process of certifying and accrediting information systems that support federal government agencies.

This document defines two very important processes: *security accreditation,* and *security certification.* Though the two terms sound very similar, they have very important distinctions that must be understood before we can discuss this document any further.

Security Accreditation: "The official management decision to authorize operation of an information system." This process involves *the assessment of risk, the development of a security plan,* and *security evaluation.* The decision to accredit an information system is made by a senior official within that agency. It is a statement saying that that official accepts the risk level of the system to the agency, and that the agreed upon set of security controls is sufficient given that level of risk. That official is then responsible not only for the security of that system, but also for any breach that may occur.

Security Certification: "The comprehensive evaluation of the management, operation, and technical security controls in an information system." This is the security evaluation that was listed as part of the security accreditation process. The security certification supports, and is a part of, the security accreditation. The security certification is the comprehensive evaluation

of the management, operational, and technical security controls in an information system. An accredited third party that is independent of the federal agency must make this certification. The certifier provides the agency official with a comprehensive report detailing the certification findings. The agency then uses that report to reassess the risks, make appropriate changes to the security plan, and make the decision whether or not to accredit the system. Circular A-130 states that it is a federal agency's responsibility to "protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information." Therefore, it is important to note that the final decision whether or not to accredit a system lies with the *agency official.* The certifying agents, though required in the process, can ultimately only point out deficiencies and make recommendations. It is up to the federal agency to act on those recommendations.

Once the accreditation and certification processes are understood, the document maps what the roles in the processes are, who fills those roles, and what their responsibilities are. It is incredibly detailed, and even includes example accreditation and certification letters that can be used.

It is worthy to note that this document will remain in its "public comment" phase until August 31, 2003. In other words, anyone in the information security field that has any input, comments, or suggestions concerning any of the material can direct those directly to the NIST.

NIST Special Publication 800-53

This document, "Guide for Selection and Specification of Security Controls for Federal Information Systems", is scheduled for release during the summer of 2003. It is the second in a series of three documents that are part of NIST SCAP. Within this document, there will be a set of minimum-security controls for low, moderate, and high risk information systems. These controls will be used in conjunction with FIPS Publication 199 to determine the required level of security for any federal agency's information systems.

The standards that will be contained in this document are to provide a baseline for federal agencies in addressing the necessary security for their information systems. Agencies will also be required to perform additional studies of their own information systems to determine if any adjustments to the baseline security model are necessary. These adjustments may include security enhancements, or they may include eliminating a requirement. Any adjustments that are made must be made based on specific threat and vulnerability information obtained during the risk assessment of the information system.

The security controls in Special Publication 800-53 will divided into three "classes". The classes are management, operational, and technical controls.

These classes are compatible with an older NIST document: NIST Special Publication 800-18. This document, published in 1998, is a guide for developing security plans for government information systems. The three classes correspond with the major sections of a security plan as defined in this document. Within each of the classes, there will be specific "families" defined that will cover the following topic areas: risk management, system development and acquisition, configuration management, system interconnection, personnel security, system interconnection, security awareness, education and training, physical and environmental protection, media protection, contingency planning, hardware and system software maintenance, system/data integrity, documentation, incident response capability, identification and authentication, logical access, audit, and communications. This document will be very comprehensive, and provide a strong baseline to assist agencies in applying appropriate levels of defense to their information systems. It should also be noted that NIST plans release of a related document, NIST Special Publication 800-60 "Guide for Mapping Types of Information And Information Systems to Security Objectives and Risk Levels", in the fall of 2003. Though not officially listed in the Phase One documents, it will be used in conjunction with those documents.

NIST Special Publication 800-53A

This document, subtitled "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems" is scheduled for release in the winter of 2003-04. It will be a companion document to SP 800-53. An agency or a certifier will be able to use the procedures in this document as a starting point to verify the effectiveness of the security controls that it deploys from SP 800-53A. It is possible, and even likely, that an agency might have special circumstances that would warrant security measures not included in SP 800-53A. Tests would need to be created by the agency or certifier in those cases.

Phase Two

Another important goal of SACP is to create a network of public and private organizations that are certified to conduct security certifications of federal agency systems. To accomplish this, there must be criteria for accrediting these organizations to conduct certifications in accordance with NIST Special Publications 800-37, 800-53, and 800-53A. (Note: This accreditation refers to an *organizational accreditation* of a certifying agent, and is different from the *security accreditation* described earlier in this paper.) There must also be proficiency tests to demonstrate the competence of the assessment organization in performing certifications. This competence should be based on the organization's mastery of the NIST guidelines contained in the Special Publications.

Phase Two is still in the early planning stages. The desire of NIST is to complete the Phase One documents before fully embarking on Phase Two. There will be public workshops at the beginning of the Phase to discuss organizational accreditation models. The NIST hopes to begin accrediting organizations by fall of 2004.

Summary and Conclusions

The SCAP will provide a detailed roadmap for federal agencies to use to meet their information security responsibilities. A very simple example of the steps an agency would take could be as follows:

- An agency determines its information security responsibilities using Circular A-130.
- An agency determines the risk factor of its information system and categorizes that system based on the risk factor using FIPS Publication 199.
- The agency comes up with a detailed security plan and applies security controls to its system using NIST Special Publications 800-18, 800-53, and 800-60.
- The agency has its system certified by an accredited third-party agent, makes necessary changes, performs necessary testing, and makes an accreditation decision. It refers to guidelines and procedures in NIST Special Publications 800-37 and 800-53A.

It is important to recognize that this is not a one-time process. Any information system is constantly changing, growing, and adapting depending on the needs of the organization using that system. Therefore, FISMA requires that an agency's information system must be periodically reviewed and accredited throughout its life cycle.

Any information security professional should closely monitor the developments of the SCAP. As these procedures are written and become standard practice within all of the federal government, it will take trained professionals to help agencies meet the requirements. It will take certifiers to evaluate the vast number of systems that will need to be accredited. Private industry will certainly begin to adopt these well-constructed guidelines and adapt them to their own businesses. An information security professional can stay on the cutting edge of their profession by keeping abreast of these policies, procedures, and guidelines. In fact, by participation in the public comment periods for the NIST documents, you can actually have a say in the direction of the field! (Those comments can be submitted via email to the Computer Security Division, NIST at sec-cert@nist.gov).

References

"Circular No. A-130—Revised." Office of Management and Budget. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (1 August 2003).

"E-Government Act of 2002." (December 2002). http://www.pubklaw.com/legis/hr2458.html (25 July 2003)

Katzen, Sally. "Office of Management and Budget. Management of Federal Information Resources." https://www.oa.doe.gov/guidedocs/9602a130/9602a130pre.html (22 August 2003).

National Information Assurance Project. "NIST Launches High Priority System Certification And Accreditation Project." 28 October 2002. http://www.niap.nist.gov/ (8 August 2002).

"The Computer Security Act Of 1987" (Public Law 100-235). 8 January 1988. http://www.house.gov/science_democrats/archive/compsec1.htm (22 August 2003).

NIST. "Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems." (May 2003). http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf (25 July 2003).

NIST. "Security Assessment Program." http://csrc.nist.gov/sec-cert/ca-assessment.html (1 August 2003).

NIST. "Security Controls." http://www-08.nist.gov/sec-cert/ca-controls.html (1 August 2003).

NIST. "Security Project Background." http://csrc.nist.gov/sec-cert/ca-background.html (1 August 2003).

NIST. "Security Project Library." http://cs-www.ncsl.nist.gov/sec-cert/ca-library.html (1 August 2003).

Ross, Ron & Swanson, Marianne. NIST. "NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems" (June 2003) .
http://www-08.nist.gov/publications/drafts/sp800-37-Draftver2.pdf (25 July 2003)

"Section 5131 of the Information Technology Management Reform Act of 1996 (CLINGER-COHEN ACT)" 5 September 2000.
http://wwwoirm.nih.gov/itmra/itmra96.html (15 August 2003).

Sehildkraut, Jeffrey. "The E-Government Act of 2002." 26 February 2003.
http://www.bls.gov/opub/cwc/print/cm20030220yb02p1.htm (1 August 2003).

Swanson, Marianne. NIST. "NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems." (December 1998).
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF (22 August 2003).

"The Paperwork Reduction Act of 1995." (1 October 1995)
http://www.cio.gov/Documents/paperwork_reduction_act_1995.html (1 August 2003).