Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

U.S. Government IT Security Laws

The introduction of computers and the Internet in private and government offices opened the doors to a complex and new world of business. This new world was full of windows of opportunities for the ill-intentioned and severally devoid of strong doors with locks. Several laws have been passed to secure those doors of ill-intent while maintaining windows for the public. One such law is the Federal Information Security and Management Act (FISMA) enacted in December 2002 as part of the E-Government Act of 2002. Since its i...

Copyright SANS Institute
Author Retains Full Rights

AD

U.S. Government IT Security Laws

A Guide to IT Security Legislation
and
Contractor Responsibilities

Trevor Burke
GIAC Security Essentials Certification (GSEC)
Coralville, Iowa (September 2003)
Practical Assignment Version 1.4b Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ABSTRACT **1**

BRIEF HISTORY OF ELECTRONIC LAW **2**

WHICH LAWS APPLY TO FEDERAL CONTRACTORS? **3**

THE PLAYERS **4**

THE FIVE COMMANDMENTS **6**

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS PUB) 199: 7
NIST SP 800-37: 7
GUIDE FOR THE SECURITY CERTIFICATION AND ACCREDITATION OF FEDERAL INFORMATION SYSTEMS 7
Initiation Phase *8*
Certification and Accreditation *9*
Continuous Monitoring Phase *9*
NIST SPECIAL PUBLICATION 800-53: 11
NIST SPECIAL PUBLICATION 800-53A: 12

LESSONS LEARNED AND CONTRACTOR RESPONSIBILITIES **12**

CONCLUSION **13**

REFERENCES **15**

© SANS Institute 2004, Author retains full rights.

Abstract

The introduction of computers and the Internet in private and government offices opened the doors to a complex and new world of business. This new world was full of windows of opportunities for the ill-intentioned and severally devoid of strong doors with locks. Several laws have been passed to secure those doors of ill-intent while maintaining windows for the public. One such law is the Federal Information Security and Management Act (FISMA). Enacted in December 2002 as part of the E-Government Act of 2002, government entities and subsequently their contractors have been hurried to comply with the law. Since its inception there have been several guidelines established to help government entities conform with FISMA.

Certification and Accreditation (C&A) is the cornerstone for federal agencies implementing the mandates under the Federal Information Security and Management Act (FISMA). C&A is not everything, however. Before a government agency or their contractor even begins working towards C&A there are several steps that should be understood and followed, including understanding who is involved, what is required, where to find information and how to use that information. Because the law is new and went into effect so quickly there is much misunderstanding and confusion both at the federal agency level and the government contractor level. This document will serve as a guide to those new to federal IT law and address the above four issues, outline the guidelines and steps to ensure successful C&A as designed by NIST, and subsequently address lessons learned from trying to comply with FISMA.

Assumption: All references to “federal”, “government”, and “agency(ies)” refer to the “United States of America.”

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Brief History of Electronic Law

The Federal Information Security Management Act (FISMA)[1] when signed into law by the President as part of the E-Government Act of 2002 permanently reauthorized and amended several previous laws. Whether it was a goal of reducing or eliminating paper waste in the government, standardizing technologies and processes, or securing our government resources, all of these laws were designed to give the federal government an upper edge in addressing the changing world of technology.

The first laws (Government Paper Reduction Act of 1980 and 1995[2] (PRA) and Government Paper Elimination Act of 1998[3] (GPEA) were meant to move the federal government from a paper-based bureaucracy, where inconsistencies across agencies led to wasted money and resources, to a "efficient, effective and economical"[4] government that shared information and resources taking advantage of technology and all it had to offer. Soon to follow were laws (Computer Security Act of 1987[5] (CSA) and The Information Technology Management Reform Act of 1996[6] (Clinger-Cohen Act)) designed to secure the federal IT infrastructure as well as emphasize "a risk-based policy for cost effective security."[7] In order to assist federal agencies comply with these laws, the Office of Management and Budget (OMB) released Circular A-130, Appendix A Security of Federal Automated Information Resources. Circular A-130 required federal agencies to:

i) "plan for security;
ii) ensure that appropriate officials are assigned security responsibility;
iii) periodically review the security controls in their information systems; and
iv) authorize system processing prior to operations and, periodically, thereafter."[8]

Specifically called out in Circular A-130, agencies must execute the accreditation process, thereby making the agency accountable for its own system, which includes completing risk assessments and security plans. Additionally, Circular A-130 introduced into law the definition of General Support System (GSS) and

---

[1] FISMA - http://csrc.nist.gov/policies/FISMA-final.pdf
[2] Paperwork Reduction Act of 1995 – http://www.cio.gov/Documents/paperwork_reduction_act_1995.html
[3] H.R 4328 – Title XVII: Government Paperwork Elimination Act of 1998 - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ277.105.pdf – and OMB Procedures and Guidance on Implementing the GPEA – http://www.whitehouse.gov/omb/memoranda/m00-10.html
[4] OMB Circular A-130, Section 5: Background – http://whitehouse.gov/omb/circulars/a130/print/a130.html
[5] Computer Security Act of 1987 – http://www.cio.gov/Documents/computer_security_act_Jan_1998.html
[6] Clinger-Cohen Act – http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html
[7] Security Certification and Accreditation Project: Background – http://csrc.nist.gov/sec-cert/ca-background.html
[8] IBID

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Major Application (MA), which will be discussed further in "Lessons Learned and Contractor Responsibilities" section of this document.

The Government Information Security Reform Act (GISRA)[9], signed into law as part of the National Defense Authorization Act of 2000, addressed the issues of program management and required further assessment and reporting of information security. This law was not permanent, however, and was scheduled to sunset in November 2001. FISMA was introduced, as part of the E-Government Act, making the provisions under GISRA permanent. The goal of FISMA, in short, is to "require each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."[10]

Which Laws Apply to Federal Contractors?

Perhaps one of the most difficult aspects of IT security and C&A is understanding which federal laws must be complied with and by whom and this is without considering local and state legislation. It could be assumed that CIOs, Security Officers and others under their direction at the federal agencies would know which laws apply and how they apply to their programs and subsequently their contractors. That is not always the case, however. The fact is there are so many Acts, presidential Executive Orders and official guidelines that it really is not so simple. Perhaps the best reference are the Acts and Executive Orders themselves because most have sections dedicated to listing the applicable and associated laws that are either superceded or act as references. That assumes though, that one already knows which laws apply and know where to find the original text and not just a summary.

The situation for federal contractors becomes a little more confusing. There are many security and IT laws in existence that appear to only address federal agencies. When the laws are read in detail, however, there is often the phrase, to use FISMA as an example: "including those provided or managed by another agency, a contractor or other source"[11] or something similar imbedded. This phrase requires federal government contractors to adhere to the same mandates as the agency for which they are working. Again, this is not a simple matter and will be discussed further in the "Lessons Learned and Contractor Responsibilities" section of this document.

In trying to determine which laws are applicable, the obvious first choice is to ask the manager, director or security officer at the agency; they should know. New information and directives are not always passed down the chain in a timely

[9] National Defense Authorization Act – http://www.cio.gov/Documents/gisra_link_to_pdf_file.html
[10] NIST SP 800-37 – 2nd Public Draft, pg. 1 – http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf
[11] Federal Information Security Management Act (FISMA) – 3544(b)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

manner, so if one wants to be prepared another good place to check is the media. There are many websites dedicated to IT information and many of these sites have sections that focus on federal regulations. These websites have become more prevalent with the recent and very quick enactment of so many laws pertaining to security since the terrorist attacks on 9/11/01.

The following non-government websites, while occasionally bias, have proven to be good sources of security legislation information:

GovExec.com (http://www.govexec.com)

The 'E-Government' link on the home page leads to a wealth of news, special reports, and links to other related web sites. There is also a "Bill Tracker" link on the home page that leads to a list of current bills going through Congress. It includes a search mechanism for bills and legislation as well as a search by ZIP Code for elected officials. In their own words, "GovExec.com is government's business news daily and the premier web site for federal managers and executives."[12]

Government Computer News (GCN) (http://www.gcn.com)

While the home page lists current news articles on government security issues, following the 'E-Government' link will provide the most concise list.

Washington Technology (http://washingtontechway.com)

Washington Technology provides links to "Budget/Policy/Legislation", "Security", "E-Government" and several other IT security topics containing current news releases and information.

Center for Democracy and Technology (http://cdt.org)

This site is a watch dog/activist site, so they are slightly biased, but they are very up-to-date on the latest IT legislation and news. "The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies."[13]

There are a plethora of other websites and news magazines spanning the political spectrum. Anybody should be able to find one that fits their information needs.

The Players

Once the applicable federal mandates have been identified, it is important to understand which agencies and entities are responsible for which pieces of the legislation. Knowing which agencies, and subsequently the audience, are

[12] GovExec.com – About Us - http://govexec.com/about.htm
[13] Center for Democracy and Technology – Mission – http://www.cdt.org/mission/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

involved in the process allows one to focus the process and documentation towards the agency making the request. It also helps in the general sense of knowing where the document and responsibilities for review and follow-ups will end up.

The Whitehouse (www.whitehouse.gov)
The President is responsible of overseeing the Executive Office of the President, which includes[14]: the Office of Management and Budget (OMB), the National Security Council, the Office of Homeland Security, the Office of Science and Technology Policy, as well as a number of other non-security and information technology related offices. These offices are primarily responsible for advising the President on issues pertaining to their areas of expertise and therefore have significant influence in policy decisions and drafting of Executive Orders.

Office of Management and Budget (OMB) (www.whitehouse.gov/omb)
OMB is required under the Paperwork Reduction Act to "develop and implement uniform and consistent information resources management policies" as well as oversee, evaluate, and measure compliance.[15] OMB is responsible of overseeing C&A and reporting the results to Congress.[16] OMB is included in the Executive Office of the President.

Commerce Department (www.commerce.gov)
The Commerce Department oversees a wide array of topics ranging from trade, economics, statistics, census, weather, and technological innovation.[17] The National Institute of Standards and Technology (NIST) is an agency of the Technology Administration of the Commerce Department.

National Institute of Standards and Technology (NIST) (www.nist.gov)
NIST is an agency of the Technology Administration of the Commerce Department. NIST is responsible for working with industry to "develop and apply technology, measurements, and standards."[18] The Computer Security Division of the NIST Information Technology Laboratory is responsible for developing information technology standards and guidance on applying these standards. NIST is charged with developing the standards and guidelines for compliance with FISMA[19] and OMB Circular A-130[20]. The 800 series[21] documents are especially important in understanding IT security guidelines and mandates including the mandates under FISMA.

Office of Electronic Government

---

[14] The Executive Office of the President – http://www.whitehouse.gov/government/eop.html
[15] OMB Circular A-130, Section 5: Background
[16] Federal Information Security Management Act (FISMA) – 3543(a)(8)
[17] U.S. Commerce Department – http://www.commerce.gov/index.html
[18] U.S. Commerce Department – NIST – http://www.commerce.gov/organization.html
[19] Federal Information Security Management Act (FISMA) – Section 303(a-d)
[20] OMB Circular A-130, Section 9c: Assignment of Responsibilities – Department of Commerce
[21] NIST Publications – http://csrc.nist.gov/publications/nistpubs/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Office of Electronic Government was created under the E-Government Act of 2002 to "improve government IT."[22] The office is part of OMB and is devoted to implementing the President's e-government agenda which includes the E-Government Act (and FISMA), the GPEA, the Clinger-Cohen Act, and others.

Federal CIO Council
The Federal CIO Council was established in 1996 by Executive Order 13011[23] and written into law under the E-Government Act of 2002. As required by E-Government Act, each federal agency must have a Chief Information Officer. The CIO Council is made up of several departments and agencies and "serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources."[24] The Deputy Director of Management at OMB chairs the CIO Council.

Congress
The House of Representatives and Senate, of course, introduce, debate, and create federal law. They also evaluate laws for effectiveness, for example, OMB must report on the implementation and status of FISMA across federal agencies.

The Five Commandments

Just as important as C&A itself are the steps before and after C&A. A series of guidelines have been developed by NIST to assist federal agencies through the entire compliance process, not just C&A. These documents outline best practices and identify standards and procedures for security controls.

The practical "Government System Certification: A Guide to Government Mandates" by Christian Enloe[25], did an excellent job in addressing the steps involved in C&A as they were written at the time and serves as a good starting point for understanding C&A. However, the guidelines have since been updated and new documents have been released.

The primary C&A documents, once fully completed and released, will consist of[26]:

- Standards for Security Categorization of Federal Information and Information Systems (FIPS Publication 199) [27]
- Guide for the Security Certification and Accreditation of Federal Information Systems (NIST Special Publication 800-37)

---

[22] CIO Magazine - "A More Perfect Union." http://www.cio.com/archive/030103/union.html
[23] CIO Council - http://www.cio.gov/index.cfm?function=councildescription&subsection=aboutthecouncil
[24] CIO Council - http://www.cio.gov/index.cfm?function=councildescription&subsection=aboutthecouncil
[25] GSEC Practical "Government System Certification: A Guide to Government Security Mandates" by Christian Enloe, December 2002. http://www.giac.org/practical/GSEC/Christian_Enloe_GSEC.pdf
[26] NIST SP 800-37 – 2nd Public Draft
[27] FIPS PUB 199 - http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Security Controls for Federal Information Systems (NIST Special Publication 800-53)
- Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems (NIST Special Publication 800-53A)
- Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels (NIST Special Publication 800-60)

These papers are considered to be in draft form until all have been thoroughly reviewed, approved, and released to the public. Currently only FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems* and NIST 800-37: *Guide for the Security Certification and Accreditations of Federal Information Systems* have been released. Once completed these five documents are "intended to provide a structured, yet flexible framework for identifying, employing, and evaluating the security controls in federal information systems"[28] and will provide the framework for complying with FISMA.

Federal Information Processing Standards Publication (FIPS PUB) 199:

Standards for Security Categorization of Federal Information and Information Systems

FIPS PUB 199 was released in draft form in May 2003. It seeks to create security categorization standards to "provide a common framework and understanding."[29]

There are three potential levels of risk (low, medium, and high) associated with each security objective (confidentiality, integrity, and availability).[30] Using the table[31] and descriptions provided in the guide, agencies can categorize their level of risk for enclosure in the System Information section of their security plan.

NIST SP 800-37:

Guide for the Security Certification and Accreditation of Federal Information Systems

NIST SP 800-37[32] was initially released in draft form in October 2002 and a second draft was released in June 2003.[33] The initial draft identified two phases:

---

[28] NIST SP 800-37 – 2nd Public Draft, pg. iv.
[29] FIPS PUB 199, pg. 2
[30] FIPS PUB 199, pg. 5
[31] FIPS PUB 199, pg. 7
[32] NIST SP 800-37 - http://csrc.nist.gov/sec-cert/ca-process.html
[33] Publications Development Schedule - http://www.csrc.nist.gov/sec-cert/ca-schedule.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Certification and Accreditation. In the second draft two other phases were identified: Initiation and Continuous Monitoring.

The NIST guidelines undergo detailed reviews by both the government and public. In response to submitted comments, the Initiation and Continuous Monitoring Phases were introduced by NIST.

Initiation Phase

The Initiation Phase of C&A is a very important one. It gives the system authorizing agent the opportunity to assess the system security plan before it goes into the Certification phase. By pre-assessing the system security plan the authorizing agent will have greatly increased the chances of successful certification and accreditation. It is like testing a hot bath with only your toe before throwing your whole body in; it is much better to assess the water before risking a full body burn.

The Initiation Phase consists of three sub-phases:[34]

- Preparation;
- Notification and Resource Identification; and
- Security Plan Analysis, Update, and Acceptance

The Preparation sub-phase is just as its name suggests, a phase where the supporting documentation for the C&A is prepared and validated by the system owner; putting your ducks in a row, so to speak. More specifically, in this phase the system security plan as well as the initial risk assessment should be reviewed to confirm vital system information has been documented. If NIST 800-18 was followed during creation of the security plan then all required information should already be part of the plan. It should be verified that the security category as established in FIPS PUB 199 is also clearly identified. All potential threats, vulnerabilities, and risks using the guidelines established in NIST SP 800-18 and NIST SP 800-30 *Risk Management Guide for Information Technology Systems* should also be clearly stated. And lastly, security controls using the guidelines in NIST SP 800-53 (when it's released), should be validated.

The Notification and Resource Identification sub-phase is a standard phase in program management. It is intended to communicate the *need* for the project, for example, C&A, the resources needed to carry it out, and the schedule of tasks and deliverables. Without this sub-phase programs could be left without the appropriate resources, such as development or documentation staff, and, in some cases more importantly, without the budget to complete the project. With any project, proper notification must be given to those who provide the resources.

[34] NIST SP 800-37, pg. 21.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

It is during the Security Plan Analysis, Update, Acceptance sub-phase that the plan should be validated against current NIST standards as outlined in NIST SP 800-18[35]. 800-18 describes in detail how to create and maintain a system security plan. Conformity with this standard is what the security plan will first be judged against in C&A. Uncompliance with the standard will flag the entire system as potentially un-certifiable. If deficiencies have been identified in the plan then, of course, it should be updated before the Certification process is started.

Certification and Accreditation

For information on the Certification and Accreditation phases, please refer to the GSEC practical "Government System Certification: A Guide to Government Mandates" by Christian Enloe. In brief, Enloe identifies and describes what it takes to pass a system review. He identifies six basic requirements[36]:

- Defining System Boundaries;
- Risk Assessment;
- Self-Assessments;
- System Security Plans;
- Contingency Plans; and
- Plan of Actions and Milestones (POA&M)

In addition to what Enloe describes in his paper, it should be noted that at this point in the entire C&A process most supporting documentation should already be created and should only need to be evaluated by the certifying authority. Corrective action plans will be created at the completion of the Certification phase usually requiring the supporting documentation to be updated before entering the Accreditation phase.

Continuous Monitoring Phase

Per FISMA, individual agencies must report on their systems on a yearly basis.[37] Additionally, as part of an agencies security program, they must make "periodic assessments of the risk"[38] of the systems. Not only are yearly or periodic checks of system security important, it should be an on-going process. C&A supporting documents, such as the security plan, risk assessment, business continuity plan and disaster recovery plans are vitally important to security; they are living documents that should be regularly updated. It is not enough to wait until the next C&A to update and amend security documentation. As living documents they can be compared to regular checkups with the doctor; skip a few visits and you could find yourself in serious trouble down the road. In order to maintain checks and

[35] See NIST Special Publication 800-18 http://www.csrc.nist.gov/sec-cert/ca-library.html
[36] GSEC Practical "Government System Certification: A Guide to Government Security Mandates" by Christian Enloe, December 2002, pg. 5.
[37] E-Government Act of 2002: Title III-Information Security-3544c1.
[38] IBID

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

controls on the system documentation and the system itself, a good configuration management plan must be established.

Configuration management plans should contain the five following sections, at a minimum:

- Executive Summary of the System;
- Roles and Responsibilities;
- Communications;
- Configuration Management Activities; and
- Resources

The Executive Summary should mirror the same information provided about the system in the security plan. It should include: system identification, the responsible organization, and an introduction, including, purpose, scope and audience. By mirroring the security plan's and CM plan's system information, a consistency has been created, validating their existence with the system as a whole.

As with any system document and project it is important to identify Roles and Responsibilities. This reduces the risk of error and negligence. This section should clearly state who is responsible what parts of configuration management. Typically this can be broken down into three groups: the CM Management Team; the CM Organization; and specific CM responsibilities.

> The CM Management group is responsible for the overall management of the business processes. This is typically senior management.
>
> The CM Organization group is responsible for addressing standard procedures and practices, including tools.
>
> Individual CM responsibilities outline exactly who is responsible for what tasks, such as opening change requests, version controlling, or approval for changes. This section should be very detailed to avoid confusion over functions.

The Communications section should describe in detail how the CM system reports, tracks and resolves change requests. This is quite often managed via automated tools.

Configuration Management activities should be clearly established and understandable. The activities can vary by organization and by tool, but they should all describe the configuration items under the projects control and what constitutes a valid change request. This section should also address the process for controlling versions, opening change requests, tracking changes, meeting schedules, implementation decisions, validation against security controls, and audits and reviews.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Similar to the security plan, resources should be identified and the proper managers consulted to ensure that the appropriate people, facilities, tools and budget are available.

In addition to configuration management, good system maintenance calls for the security controls to be monitored for effectiveness. As technology changes and threats mutate the security controls need to be re-evaluated and then evaluated again. This can be a costly process, so for federal systems the guidelines call for the identification of a subset of controls to limit scope.[39] NIST SP 800-53 assists agencies in identifying which subset of security controls to evaluate and monitor. After the appropriate security controls have been identified the must be monitored for their effectiveness. NIST SP 800-53A identifies techniques and procedures for verifying security controls.

When changes are made to the system and either the system itself changes or the security controls change, the security plan and other supporting documentation must be updated. The schedule for releases is determined by individual agencies and by project, but generally it would be a good idea for large systems to update the supporting documentation as changes occur and subsequently distribute the plans at least quarterly.

Lastly, status reports to the authorizing official should identify on-going activities, any updates to supporting documentation, and should include a plan of action and milestones.[40]

NIST Special Publication 800-53:
Guide for the Selection and Specification of Security Controls for Federal Information Systems

NIST SP 800-53 has not yet been released for public review. The NIST C&A website,[41] however, states that this guide will "establish a set of minimum security controls for low, moderate, and high risk information systems. These predefined sets of security controls provide a baseline, or starting point, for agencies in addressing the necessary safeguards and countermeasures required for their information systems."[42] Adjustments to the baseline set of controls will be allowed but any differences must be clearly stated in the system's security plan. "Upon completion of the security control process (which is part of the Continuous Monitoring phase of the C&A) the agreed upon set of controls, taken together, should satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its

[39] NIST SP 800-37, pg. 37
[40] IBID
[41] Security Controls – http://csrc.nist.gov/sec-cert/ca-controls.html
[42] IBID

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

information."[43] The initial public draft of NIST SP 800-53 is scheduled for release in September 2003.

NIST Special Publication 800-53A:

Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems

NIST SP 800-53A has not yet been released for public review. The NIST C&A website[44] states that this guide will "establish a set of techniques and procedures to verify the effectiveness of security controls listed in NIST SP 800-53."[45] Anticipated techniques to be included in verification process include:

- "Interviewing agency personnel associated with the security aspects of the system;
- Reviewing and examining security-related policies, procedures, and documentation;
- Observing security-related activities and operations;
- Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations; and
- Conducting demonstrations and exercises."[46]

Much of what will come out of NIST SP 800-53A is likely to be fairly standard for monitoring the effects of security controls at various government agencies and private companies currently. However, these techniques and procedures will help verify that all groups following these guidelines are validating their systems using the same or at least very similar criteria, making the C&A process more "consistent, comparable and repeatable."[47]

Lessons Learned and Contractor Responsibilities

More often than not, federal contracts have been designed with security and information-sharing spelled out; it is clear who owns what pieces of information and what must be delivered to the government. However, given privacy and proprietary laws it is not as clear-cut as a contractor just handing over their security documentation to an agency. Security plans, business continuity plans, disaster recovery plans, risk assessments, etc. all contain highly sensitive information that should only be accessed by a few individuals in a private company let alone handed over to an agency for evaluation and review. Add to this that many agencies use multiple contractors to handle their IT work. For example, an agency could have one contractor responsible for development and management of a software project, such as a website, but have a different

[43] Security Controls – http://csrc.nist.gov/sec-cert/ca-controls.html
[44] Verification Techniques and Procedures – http://csrc.nist.gov/sec-cert/ca-verification.html
[45] IBID
[46] IBID
[47] IBID

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

contractor responsible for housing and managing the infrastructure, such as servers, mainframes, T1 lines, etc. As part of C&A and compliance with FISMA, an agency will be required to provide a business continuity plan for the system. How do they accomplish this when the information is proprietary to each contractor and the contractors are less than willing to share that information with each other?

This issue has been made more confusing by identifying systems as either General Support Systems (GSS) or Major Applications (MA) and requiring separate documentation for each, as dictated in Circular A-130.[48] A GSS is an "interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people." A MA is defined as an "application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized, access to or modification of the information in the application." Isolating and categorizing these two systems creates a major disparity of information when agencies are working with multiple contractors.

Consider the example above where a GSS is in control of the hardware and the MA is in control of the application and its interfaces. If a GSS facility is completely wiped out and they move to their hot site, how do the GSS and MA quickly get back online and communicating when they have not shared and coordinated their disaster recovery or business continuity plans? This leaves the agency at risk.

Contractually it is likely in the agency's authority to request both the GSS and MAs proprietary security documentation separately, eliminating the issue of sharing proprietary information between one contractor and the agency, but it does not solve this issue of communication and coordination between contractors. While the burden of splicing the documents into all encompassing plans might be accomplished by the agency, this burden is often overwhelming because of a lack of resources and knowledge within the agency. Moreover, once the all encompassing plan is created by the agency, it could not be shared with the contractors who, in the event of a disaster, would be tasked with recovery. This is quite likely to be a confusing issue for some time with no clear solution.

Conclusion

With the ever-changing world of technology comes the ever-presence of threats. And with the increase in threats comes legislation to deal with those threats both at government and private company levels. Federal IT legislation has evolved considerable over the last 20 years and will, of course, continue to evolve. The challenge for government agencies and their contractors will be in knowing which

[48] OMB Circular A-130, Appendix II: Definitions

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

laws are applicable, understanding the applicable laws and then finding the assistance in fulfilling the requirements dictated under those laws. As it currently stands NIST is charged with designing the guidelines and providing the assistance to agencies. Once the full five guidelines are released agencies will have in their hands a wealth of information and tools in assisting them with not only C&A but the laws themselves.

It will be up to the agencies how they use these guidelines and address them in response to their contractors. And while they provide the means for consistency and repeatability across and within agencies there is still work to be done. Efforts need to be made to answer the question of communication between contractors. The issue of sharing proprietary security information between agency and contractors needs to be assessed; additionally, FISMA is still very young and needs to be rigorously evaluated. In the coming months, agencies, their programs, and their contractors will be going through the C&A process and most will be going through it for the first time. This process will create many questions and issues and will, in turn, require the guidelines and perhaps even the laws requiring the guidelines to be re-evaluated. Security holes in systems will no doubt be identified and need to be dealt with; this will cost money.

The original E-Government bill in 2001 called for $100 million over 3 years, however, OMB only received $5 million for 2003 and will only receive $5 million for 2004[49]. It remains to be seen whether this will be enough for the government and does not consider the implications to changes in security for contractors and then in turn the increase in costs of using those contractors. While this is far outside of the scope of this document, it is nonetheless worth noting when understanding the federal government's challenges in living up to the requirements of and the legislation aimed at managing IT security.

[49] Washington Post – "No Stellar E-Gov Funding" - http://www.washingtonpost.com/wp-dyn/articles/A60315-2003Sep11.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. Ross, Ron. Swanson, Marianne. "Guide for the Security Certification and Accreditation of Federal Information Systems." NIST Special Publication 800-37 – 2nd Public Draft – June 2003. URL: http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf (24 Sept. 2003).

2. U.S. House of Representatives. "Electronic Government Act of 2002: *Federal Information System Management Act.*" H.R. 2458 – 107th Congress. 17 Dec. 2002. URL: http://csrc.nist.gov/policies/FISMA-final.pdf (24 Sept. 2003).

3. U.S. Senate. "Paperwork Reduction Act of 1995." S. 244 – 104th Congress. 14 Feb. 1995. URL: http://www.cio.gov/Documents/paperwork_reduction_act_1995.html (24 Sept. 2003).

4. U.S. House of Representatives. "Title XVII: Government Paperwork Elimination Act of 1998" H.R. 4328 – 105th Congress. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ277.105.pdf (25 Sept. 2003).

5. U.S. Office of Management and Budget. "OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act." Memorandum 00-10. 25 April 2000. URL: http://www.whitehouse.gov/omb/memoranda/m00-10.html (24 Sept. 2003).

6. U.S. Office of Management and Budget. "Circular No. A-130" Revised. 8 Feb. 1996. URL: http://whitehouse.gov/omb/circulars/a130/print/a130.html (25 Sept. 2003).

7. U.S. House of Representatives. "Computer Security Act of 1987" H.R. 145 – 100th Congress. URL: http://www.cio.gov/Documents/computer_security_act_Jan_1998.html (25 Sept. 2003).

8. U.S. Senate. "National Defense Authorization Act for Fiscal Year 1996. *Division E: Information Technology Management Reform (Clinger-Cohen Act).*" S. 1124 – 104th Congress. URL: http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html (25 Sept. 2003).

9. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Background.*" URL: http://csrc.nist.gov/sec-cert/ca-background.html (25 Sept. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

10. U.S. House of Representatives. "National Defense Authorization Act for Fiscal Year 2001: *Government Information Security Act.*" H.R. 4205 – 106th Congress. URL: http://www.cio.gov/Documents/gisra_link_to_pdf_file.html (25 Sept. 2003).

11. "GovExec.com: *About Us*" URL: http://govexec.com/about.htm (25 Sept. 2003).

12. "Center for Democracy and Technology: *Mission*" URL: http://www.cdt.org/mission/ (25 Sept. 2003).

13. "The Executive Office of the President" URL: http://www.whitehouse.gov/government/eop.html (25 Sept. 2003).

14. "U.S. Commerce Department" URL: http://www.commerce.gov/index.html (25 Sept. 2003).

15. "U.S. Commerce Department: *Commerce Organization*" URL: http://www.commerce.gov/organization.html (25 Sept. 2003).

16. National Institute of Standards and Technology – Computer Security Resource Center. "NIST Special Publications." URL: http://csrc.nist.gov/publications/nistpubs/ (26 Sept. 2003).

17. Datz, Todd. "A More Perfect Union." CIO Magazine. 1 Mar. 2003. URL: http://www.cio.com/archive/030103/union.html (26 Sept. 2003).

18. "About the Chief Information Officers Council." CIO Council. URL: http://www.cio.gov/index.cfm?function=councildescription&subsection=aboutthecouncil (26 Sept. 2003).

19. Enloe, Christian. "Government System Certification: *A Guide to Government Security Mandates.*" December 2002. URL: http://www.giac.org/practical/GSEC/Christian_Enloe_GSEC.pdf (25 Sept. 2003).

20. National Institute of Standards and Technology. Computer Security Division. "Standards for Security Categorization of Federal Information and Information Systems." Federal Information Processing Standards Publication 199. URL: http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf (25 Sept. 2003).

21. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Security Certification and Accreditation Process.*" URL: http://csrc.nist.gov/sec-cert/ca-process.html (25 Sept. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

22. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Schedule*." URL: http://www.csrc.nist.gov/sec-cert/ca-schedule.html (25 Sept. 2003).

23. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Library*." URL: http://www.csrc.nist.gov/sec-cert/ca-library.html (25 Sept. 2003).

24. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Security Controls*." URL: http://csrc.nist.gov/sec-cert/ca-controls.html (25 Sept. 2003).

25. National Institute of Standards and Technology – Computer Security Resource Center. "Security Certification and Accreditation Project: *Verification Techniques and Procedures*." URL: http://csrc.nist.gov/sec-cert/ca-verification.html (25 Sept. 2003).

26. Webb, Cynthia. "No Stellar E-Gov Funding." The Washington Post. *Government IT Review*. 11 Sept. 2003. URL: http://www.washingtonpost.com/wp-dyn/articles/A60315-2003Sep11.html (25 Sept. 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced