Global Information Assurance Certification Paper

Building A FISMA Compliant IT Security Program In One Year

Fredric L. Everett

February 23, 2005

GIAC Security Essentials Certification Version 1.4c

Building A FISMA Compliant IT Security Program In One Year

Table of Contents

Abstract

Historically, IT security was often viewed as an add-on or stand alone activity. Few system developers, and for that fact, organizations who deployed the systems, thought to design security into IT systems and programs. Security often lost out as organizations were usually more concerned about maintaining or improving functionality. This trend of thought would soon change as Title III of the E-Government Act of 2002 removed the sunset imposed by the Government Information Security Reform Act (GISRA) and renamed it the Federal Information Security Management Act (FISMA). FISMA requires agencies or organizations (contractors or otherwise) which process federal information to demonstrate progress in meeting a number of security guidelines. Every year, each agency or organization is graded (A through F) on how well they stand with their overall FISMA compliance efforts, and are required to demonstrate improvements they have made in security versus the pervious year

Due to the importance and immediacy of FISMA, attention needs to be focused from all levels within an agency or organization. This includes senior management, the everyday user and everyone in between. But where should the agency or organization begin? The requirements for FISMA are clearly outlined, but which should be tackled first? For a best-practices management approach, it may help to group all of the FISMA requirements into four areas. Agencies and organizations should focus on the following guidelines and become FISMA compliant in one year:

- *Asset Inventory* - To know what needs protection, the agency or organization must know all of the "pieces and parts" which make up their IT systems, as well as the systems to which they interconnect.
- *Agency-wide security program* – All employees, contractors, and interns use agency or organization provided IT therefore they have a responsibility for security. The agency or organization must implement and enforce appropriate security policies and procedures according to security requirements.
- *Ensure compliance* – Conduct periodic testing and reviews to provide assurance that polices, procedures, products, and people are consistently meeting security requirements.
- *Independent Evaluations/Reporting* - Ensure accurate reporting of FISMA required metrics, as well as incorporate any audit findings to improve the security posture.

Background

Using today's standards, computer systems of yesterday were not what would be considered secure. This was due to the fact that the primary focus of computer systems was on the hardware and software design and achieving functionality. The military was one of the initial implementers of computer technology and had reasonably effective physical and personnel security. This physical and personnel security restricted system access only for those persons with the proper clearance and the "need to know". With the advent of resource-sharing computer systems that distributed capabilities and components of the computer among several users or tasks, a new dimension was added to the basic problem of safeguarding computer-resident information: How do you protect the information? Ironically, this problem was not new for information protection in general. This issue had been encountered since the invent of information that needed to be protected – how should the information be handled and secured? Now that this information had moved from document (hard-copy) to electronic (soft-copy) form, there were new challenges on the horizon.

Historically, IT security was often view as an add-on or stand alone activity. Few system developers, as well as organizations who deployed the systems, thought to design security into IT systems and programs. Security lost out as organizations were usually more concerned about maintaining or improving functionality. The emphasis was often on delivering a product or service to the customer, and information security was perceived to slow down the process of service delivery. If it didn't slow down the delivery, it was perceived to limit performance or features. (Symantec, 2002) As time passed, and the need to provide protections (mainly technical) to systems grew, the controls were often implemented and designed based upon the "non-malicious" user concept. This concept was predicated upon the assumption that none of the user population would attempt malicious, concerted efforts to circumvent security controls (Whitmore, 1973). Things have really progressed and changed since this concept was conceived.

Congress declared that improving the security and privacy of sensitive information in federal computer systems was in the best interest of the public by enacting a law called the Computer Security Act of 1987. This law created a means for establishing minimum acceptable security practices for IT systems, without limiting the scope of security measures that agencies or organizations already planned or had in use.

Under the Computer Security Act of 1987, each federal agency, or organization processing federal information, was required to provide for mandatory periodic training in computer security awareness and accepted computer security practices. This was to be provided of all employees who were involved with the management, use, or operation of each federal computer system within or under the supervision of that agency or organization. Also under this law, the National Institute for Standards and Technology (NIST), a division of the Department of Commerce, was responsible for the security of unclassified, non-military government computer systems. The law also

provided provisions for the National Security Agency (NSA) to providing technical assistance to NIST with developing security standards for the civilian security realm. Congress did not grant this authority solely to the NSA, because it felt that it was inappropriate for a military intelligence agency to have control over the dissemination of unclassified information (Mofteff, 2004).

In October 2000 the Government Information Security Reform Act (GISRA) was passed by Congress to further provide federal managers with tools to protect their assets and information. GISRA required agencies and organizations to assess the security of their information systems and report the deficiencies found. GISRA was the first piece of legislation to address information security oversight and management for the federal government as a whole by mandating security requirements, periodic reporting, accountability, and compliance. Since the days of the Computer Security Act of 1987, there were few consequences for noncompliance to information security legislation. GISRA linked budgets to compliance, which meant reduced funding for agencies who did not comply with its requirements. In other words, GISRA helped agencies and organizations achieve consistency. This piece of legislation was a strong signal from Congress that computer security was serious business. Security was finally moving to the forefront, but GISRA was scheduled for sunset late in 2002, what was to follow? (Symantec, 2002).

Title III of the E-Government Act of 2002 (signed December 2002) removed the sunset imposed by GISRA and renamed it FISMA (Federal Information Security Management Act). FISMA followed in the footsteps of GISRA by permanently authorizing and strengthening the requirements set forth by GISRA. FISMA provided a framework for government agencies to improve their security and risk management processes. Since its inception, FISMA has had an enormous effect on agency or organization's IT processes, procedures, and risk management strategies because it makes them more accountable for implementing defensible security measures and requires greater reporting on these security activities. A challenge that many agencies and organizations claim to face is that FISMA is a too high-level framework that does not offer specific solutions to meeting its requirements. FISMA is intentionally subjective as it allows room for interpretation of its many requirements and therefore requires the use of educated judgment to achieve compliance. FISMA applies to both information and information systems used by agencies, contractors, and other organizations and sources that possess or use federal information (Symantec, 2002).

Contrary to popular belief, IT security is more than having an enormous IT budget that can support the unlimited acquisition of various technological products. FISMA does not outline that the organization with the biggest IT security budget will be the most secure. Of course it would be nice to have an unlimited IT budget, but there would still be a deficiency if the organization does not have an effective management process in place. This was duly noted in a 2001 report to Congress by the Office of Management and Budget, which stated, "GISRA recognizes that while security has a technical component, it is at its core, an essential management function" (OMB "FY 2001 Report to Congress on Government Information Security Reform," Section III, page 8.) Congress further reiterated the point in 2002 by stating that "…spending more on IT

security does not always improve IT security performance. Rather, the key is effectively incorporating IT security in project and agency management actions." (Using Metrics to Improve Security, 2004).

FISMA requires each agency or organization to manage an Information Security Program that regularly assesses its state of risk and takes continual measures to reduce that risk. To ensure that management officials are held accountable for their results, FISMA requires creation of regular reports that identifies the security posture and includes a Plan of Action and Milestones for correcting high-risk situations. In addition, each agency must notify its Inspector General of any material weaknesses in its security posture, and provide a plan for eliminating these weaknesses (Principles and Challenges…, 2003).

Given these requirements that derive themselves from public law, and state that every organization that uses federal information must be compliant, it is no wonder that the first question that is often asked is "Why do organizations find FISMA compliance difficult to obtain"? There are a variety of answers to this question; however, research has shown that it can be boiled down to one response: "Agencies and organizations do not know what they do not know. And because they do not know, they do not know what they need to do". When there are so many requirements, where do you even begin? FISMA has broad and far reaching implications for every agency or organization. Trying to effectively addressing each of the key mandates (Security Program and Assessments, Policy & Procedure, Compliance, Reporting, Implementation and Independent Evaluation) is a huge task.

If FISMA compliance was simply about requiring all employees to attend a Security and Awareness training session, all agencies and organizations would be FISMA compliant. However the requirements are a bit more involved than that. Not only must agencies collect, analyze, and process the information needed to demonstrate FISMA compliance, but they must also follow up on a regular basis to ensure that milestones are met and that the state of information security is continually improved. In today's work of "do more with less" this is often a challenge as there has been reduction in staff sizes as well as funding to help accomplish these things.

Methodology

FISMA echoes the message that IT security can only be cost effective and successful when it is an integral component of strategic planning, budgeting, decision making, and performance measures. To put this in other terms, this means that security needs to be involved in all phases of the System Life Cycle. NIST outlined how security should be addressed in the System Life Cycle in their Special Publication 800-64.

Through lessons learned, industry has found that including security early in the IT system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to a system that is already operational (NIST SP 800-64). An analogy of IT security and an IT system would be a person at an automobile

dealership anticipating the purchase of a new car. At the time of purchase, the customer has the opportunity to include features such as fog lights and a sun roof. On a variety of vehicles, these are standard features and are included in the price. On other vehicles, these are "options" and cost extra. If the purchaser initially declines these "options" at the time of purchase, he/she has the ability to go to an aftermarket body shop, or return to the original place of purchase to have these options installed at a later date and time. Once the vehicle leaves the showroom, it has the potential to be operated and exposed to elements which could potentially slightly warp the sheet metal of the vehicle (snow, hail, extreme heat, etc.). Who knows, maybe the installation of the 'options', such as a sunroof may prove to be a success at a later time. At the same time, maybe because the sunroof was not originally designed into the vehicle, things may not truly fit and there may leaks in the roof. The same scenario applies for IT security. Security features could be built in from the beginning and considered throughout all phases of the life cycle, as well as security could be considered in subsequent phases of the life cycle. However, after years of operation and maintenance (applying patches, installing/uninstalling hardware/software, etc.) the new security features may not truly "fit" or be compatible with the existing configuration.

Getting Started

Due to the importance and immediacy of FISMA, attention needs to be focused from all levels within an agency or organization. This includes senior management, the everyday user and everyone in between. But where should the agency or organization begin? It is clear that security should always be considered, the requirements for FISMA are clearly outlined, but which should be tackled first? For a best-practices management approach, it may help to group all of the FISMA requirements into four areas. Agencies and organizations should focus on the following guidelines:

- *Asset Inventory* - To know what needs protection, the agency or organization must know all of the "pieces and parts" which make up their IT systems, as well as the systems to which they interconnect.
- *Agency-wide security program* – All employees, contractors, and interns use agency or organization provided IT therefore they have a responsibility for security. The agency or organization must implement and enforce appropriate security policies and procedures according to security requirements.
- *Ensure compliance* – Conduct periodic testing and reviews to provide assurance that polices, procedures, products, and people are consistently meeting security requirements.
- *Independent Evaluations/Reporting* - Ensure accurate reporting of FISMA required metrics, as well as incorporate any audit findings to improve the security posture.

Federal Information Processing Standards 199 (FIPS 199) begins the journey to FISMA compliance by requiring agencies and organizations to categorize information systems based on the objectives of providing appropriate levels of information security

according to a range of risk levels. This focus is concentrated on the impact of loss to the agency or organization with regards to Confidentiality (unauthorized disclosure), Integrity (unauthorized manipulation), or Availability (unauthorized disruption). To really understand the impact to confidentiality, integrity, or availability, the agency or organization must have a firm grasp of all the systems that it has on its network, this would be called an asset inventory. This inventory should not only include the agency's systems, but also should include the interfaces between each system and all other systems and networks, including those NOT operated by or under the control of the agency (system interconnections) (FIPS 199).

Once the criticality of the system has been determined, an accurate review of the system properties or security requirements will be identified. These requirements often start off at a high-level, but quickly gain specificity as security is further discussed. One method often used (but not mandatory) to develop and express security requirements and specification is the Common Criteria. The Common Criteria for Information Technology Security Evaluation, created by the International Organization for Standardization (ISO) provides a standard vocabulary and format for expressing the security requirements of a system (FIPS 199).

Asset Inventory

Without a solid understanding of the systems to be protected, where they are physically located, and how important they are to the agency (FIPS 199), a security program (no matter how thorough it looks on paper), will not succeed.

An IT system inventory is a comprehensive list of all IT systems in the operating unit. It contains IT security program information on each system, and provides a summary of the "pieces and parts" associated with the system. Each "piece and part" can only be associated with ONE system. It is not a good idea to have resources with co-owners. Co-ownership might prove useful in sharing the initial cost of purchase of the equipment, but just like two brothers who believe it a good idea to purchase a vehicle together, when it is time for maintenance or if there are huge repair cost, who is responsible? Having only one owner for a piece of equipment is essential for IT security administrators, in that if there is an incident involving a piece of IT computing resource or there is maintenance that needs to be performed, the appropriate party will be contacted.

FISMA requires that a complete and accurate inventory be produced for all IT systems. This requirement is echoed by the Clinger-Cohen Act, and the Office of Management and Budget Circular A-11 which require that each IT system is tracked and linked to IT capital planning, architecture, and investment control by a unique system identifier (name and/or number) (DOC, 2004).

As organizations work to complete their system inventories, a major question that surfaces deals with what is required. What does Congress require be included in the inventory? The inventory includes the IT security program information for all IT systems in the operating unit, and includes information such as:

- The unique descriptive name (identifier) for each IT system
- Sensitivity Type
- System's physical location
- Type of system (major application or general support system)
- Phase of the system life cycle
- Deactivation date (if applicable)
- Criticality level (national mission critical, mission critical or business essential)
- Exhibit 53/300 Account Code(s)
- System Impact Level (high, moderate (medium), or low)
- Operational relationships (government or contractor)
- System responsibility contact information
- System interconnections

Although this is not an all inclusive list of what may be required for a system inventory, it provides a very good reference for the types of information that effectively describes the system. The organization should maintain an up to date copy of this documentation which shows the security status of every system. The information should be updated at least annually and when significant changes occur to the status of the mission, the individual system, or system responsibility contacts (DOC, 2004).

Agency-wide security program

FISMA requires each federal agency, or organization processing federal information, to develop, document, and implement an agency-wide 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.

According to NIST Special Publication 800-50, a successful IT security program consists of:

- Developing IT security policy that reflects business needs,
- Outlining and informing users of their IT security responsibilities,
- Establishing procedures for monitoring and reviewing the IT security program after it has been implemented.

IT security is not just the responsibility of individuals with major security responsibilities. Everyone who uses an agency or organization's IT has a security responsibility. The message should be communicated from the top (management levels) of the
organization of the importance of security and should be focused on the entire user population. Jean Jacques Rousseau believed that people are naturally good, but that civilization and institutions make them evil. If we believe this, then having the head of the agency or organization (which is an institution) support something would influence the behavior of its members. Management has an important responsibility to set the

tone that the agency or organization users will follow. At the same time the security programs should be implemented from the bottom up. Users need to feel a part of the program and not that they are being dictated "dos and don'ts" which they must follow.

A key tool of the IT security program revolves around the organization's rules of behavior or acceptable use document. This outlines the acceptable behavior for the use of the organization IT. It also outlines repercussions and penalties that will be enforced due to non-compliance of users to the rules of behavior. For example, many rules of behaviors often include a statement that allows users "limited personal use" of resources such as the Internet. Unfortunately, without monitoring the actions of the users, often this "limited personal use" can become "limited TO personal use". Everyone must be held accountable for their actions. The rules should come directly from the agency or organization's policy and should apply to everyone.

Probably the most important part of implementing the IT security plan revolves around communication. If the program's implementation is not fully explained to the organization, buy-in and the necessary commitment from the users may not be possible. This communication should not occur over night. There may be push-back if users were to arrive to work one day and experienced technical difficulties that were implemented overnight that restricted what were once considered "normal" activities (NIST SP 800-50, 2003).

Ensure Compliance

Compliance with the Agency's/organization's security policies, procedures, and standards is mandatory for yearly reporting to Congress, and should be tested on a periodic basis throughout the course of the year to ensure that things written on paper is actually reality. Compliance measurement and reporting should be conducted by competent and capable staff to ensure that the defined controls are operating effectively. As with the other requirements of FISMA, there are several inherent challenges associated with this mandate, including:

1. Most agencies may not have a large or experienced IT audit function to regularly check for compliance with their established FISMA policies. This often requires staff with other responsibilities to have to perform audit/security related functions.

2. Particular attention must be paid to reporting consistency. Differences in the security skills of an organization's staff can result in inconsistent compliance reports. For example, the auditing of server identification and authentication controls conducted by two different people with varying levels of knowledge, sets of tools and experiences could result in two very distinct sets of results.

3. Auditing every single device within the network for compliance to NIST control standards is a largely manual task. There are a number of tools available that if implemented could possibly reduce costs of performing this task, such as hiring

outside contractors to perform the manual audits, reduce time to audit (overtime), as well as increase overall audit efficiency. Acquiring these tools may require monetary resources, which may introduce other challenges if budgets can not support the acquisition of new equipment.

4. Networked environments are constantly changing. The operating environment deployed today, may be very different from the operating environment being used next year. New hardware and software is constantly being installed and attention should be given to ensure that no adverse changes occur to the operating environment (configuration management).

   For example, if an organization were to consider ensuring compliance for their networks, they would have to approach it from two very distinct points of view regarding inspection: *Externally and Internally*.

   External Compliance Example: It seems as if every month IT vendors are issuing, updates, patches and "hot Fixes" to keep pace with newly discovered security vulnerabilities, worms or viruses. An organization may have a policy that states: "All Devices must be patched to the latest patch level". This could be a challenge as new updates, patches, and "hot fixes" are made available and there is a shortage of trained and qualified security staff in the organization to apply these corrections (Preventsys, 2004).

   Internal Compliance Example: FISMA compliance requires that all services, applications and programs must be assessed and accounted for on a periodic basis. For example, users (if they have administrative privileges) may install services or applications without the IT department's knowledge. Many times these programs are not approved and tested in accordance with the organization's policy. The organization would need to implement procedures (manual or automatic) that would detect the existence of unapproved software and assure compliance with this policy (Preventsys, 2004).

The consistency and timeliness of compliance reporting will be a continuous and growing need. Security is an ongoing challenge, so FISMA requires federal agencies to conduct periodic tests of security compliance (Preventsys, 2004).

Independent Evaluations/Reporting

As a part of compliance, FISMA requires that each year a independent evaluation of the Information Security program and practices must be performed. This will help the agency or organization determine the effectiveness of such programs and practices. Mandates of FISMA require the testing of internal controls and assessment of compliance.

As agencies are managing simultaneous, ongoing activities (developing and maintaining the security program, continuously monitoring the environment, testing

internal compliance, and even eliminating POA&M items) it will also need to allow an external auditor to evaluate the entire process. Independent evaluation is important to maintaining objective results and the status of the security of an IT system. If the organization has been diligent and honest in its internal compliance measures, there will not be many, if any, new Independent Evaluator findings. If there are findings, it may be difficult to view this as good thing. The Independent Evaluator should be viewed as an agency's or organization's "friend" who doesn't mind telling the true complete story. It is better for the Independent Evaluator find an area needing attention (vulnerability), than for an attacker or a person with mal intent to find the weakness and exploit it. If the latter were to occur, there is no telling what the outcome of that exploitation could be: loss of data (confidentiality, integrity, and availability), loss/disruption of service, monetary loss, damage to reputation, or loss of life (Using Metrics to Improve Security, 2004).

Being FISMA compliant is great, but it is even greater if credit is given for all the hard work put into achieving compliance. There are annual reports that are submitted to Congress tell of the agency's or organization's progress on topics such as compliance, remediation efforts and staff efficiency. Creating and managing these annual reports to demonstrate consistent progress and remediation improvement is a comprehensive task for all, and includes a number of considerations, such as:

1. The amount of data collected from continuous assessments may be overwhelming and lend itself to difficult in ensuring consistency. Agencies will have to develop processes and procedures for the collecting and reporting of data in an organized manner.

2. It is essential to maintain the security of the audit data and the integrity of the reports. Only authorized personnel with the proper access and the need-to-know should have access to this data. If the data is stored electronically, it may also need to be encrypted.

3. Plans of Actions and Milestones (remediation) reporting is very important. Per FISMA, the organization must identify all issues and corresponding remediation actions, and report on these corrective actions over time. These plans should include the issue, who is responsible for the remediation of the issue, and by what methods or means will the issue be resolved. Also, there needs to be some sort of documentation of the expected timeframe of completion of the issue. Having a well documented POA&M documents will demonstrate that the organization is implementing proper measures and processes to address identified risks in an appropriate manner (personnel, resources, time, etc.).

The annual reports give the agency or organization the opportunity to show its progress with regard to implementing effective policies and procedures. Agencies and organizations should take credit for their hard work and should produce comprehensive reports that include completeness of data collection, focused analysis, and planned remediation efforts (Preventsys, 2004).

Reporting has been improving. In the past, organizations that had not completed their asset inventories got “dinged” a full grade for that. That in turn, leads to more and more agencies completing at least that portion of the FISMA requirement. The trend had been for agencies to have multiyear technology efforts, and that are addressing computer security programs when they are replacing existing technology. This is not very effective and agencies are looking for a more rapid means to achieve FISMA compliance (Miller, 2005).

Conclusion

Unfortunately, there is no one-size-fits-all approach that can be applied to ensure FISMA compliance. For managers of information technology, FISMA has proved to be one of the most challenging pieces of federal legislation to be enacted in recent years. FISMA imposes strong requirements to improve the security of government information. It also holds agencies fully accountable for their success in meeting this goal. It should be understood that FISMA compliance is not about eliminating all risk to an organization’s IT systems. It is understood that this is impossible. Since this is the case, FISMA compliance is all about demonstrating awareness and understanding of the risks facing an organization, and implementing practices to mitigate these risks to an acceptable level for operation.

Completing the four tasks outlined in this document will reap many benefits for any organization, including, but not limited to:

- Developing a security baseline which will be useful in tracking progress in subsequent years,
- Focusing security throughout all phases of the System Life Cycle,
- Integrating security throughout the agency/organization environment ,
- Achieving compliance with FISMA requirements in one year.

References

Computer Security Act of 1987. January 8, 1988. 23 Feb. 2005 <http://www.house.gov/science_democrats/archive/compsec1.htm>>

Department of Commerce. "US Department of Commerce Process Guidance and Minimum Implementation Standards for IT System Inventory Management." 28 July 2004. 23 Feb 2005 <http://www.osec.doc.gov/cio/oipr/ITSEC/DOC%20PGMIS%20-%20IT_System_%20Inventory_Mgmt.pdf>

E-Government Act of 2002. 2002. 23 Feb. 2005 <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR02458:@@@L&summ2=m&>

"Government Information Security Reform Act" 2000. 23 Feb 2005. <http://csrc.nist.gov/policies/Subtitle-G2.pdf>

Miller, Jason. "Agency IT security improves only slightly, Congress says." Government Computer News. 16 Feb. 2005. 23 Feb. 2005 <http://www.gcn.com/vol1_no1/daily-updates/35092-1.html>

Moteff, John. "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives." April 16, 2004. 23 Feb. 2005 <www.fas.org/irp/crs/RL32357.pdf >

National Institute of Standards and Technology. "Federal Information Processing Standards 199 – Standards for Security Categorization of Federal Information and Information Systems." December 2003. 23 Feb. 2005 <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

National Institute of Standards and Technology. "Special Publication 800-50 Building and Information Technology Security Awareness and Training Program." October 2003. 23 Feb. 2005 <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

National Institute of Standards and Technology. "Special Publication 800-64 Security Considerations in the Information System Development Life Cycle." June 2004. 23 Feb. 2005 <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>

OMB A-130 Appendix III. "Security of Federal Automated Information Resources." 23 Feb. 2005 <http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html>

Principles and Challenges of the Federal Information Security Management Act. 2003 23 Feb. 2005 <http://www1.netsec.net/content/securitybrief/archive/2003-08_FISMA_Principles_Challenges.pdf>

Preventsys. "Making The Grade: A Framework for FISMA Compliance." 2004. 23 Feb.

2005 <www.preventsys.com/home/resources/>

Ross, Ron. Spring 2004. 23 Feb. 2005 “The New FISMA Standards and Guidelines.” <http://www.secure-biz.net/Spring2004/whitepapers/fisma-article-v15.doc>

Symantec. “Symantec IT Security Spotlight, Security Solutions for Federal Government.” Fall 2002 Volume 1 Edition 3. 23 Feb. 2005 <http://enterprisesecurity.symantec.com/publicsector/displaypdf.cfm?pdfid=3&PID=12557590&EID=0>

“Using Metrics to Improve Security.” NetSec Secrity Brief. September 2004. 23 Feb. 2005 <http://www1.netsec.net/content/securitybrief/archive/2004-09_Metrics.pdf>

Whitmore, Jerold, et al. Design for MULTICS Security Enhancements. Air Force Systems Command, 1973.

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event