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.

Sensitive But Unclassified

Information that is sensitive may or may not have a label such as SBU or "Eyes Only". For the person responsible for putting together a security policy, determining what information is sensitive and what may be published will be one of the most challenging aspects of the process. In this report, one will learn about the differences between classified and unclassified information. One will also learn about the many names by which sensitive information may be labeled. The history of the United States laws that affect the...

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

Sensitive But Unclassified

By

Andrew Helyer

For

SANS Institute, Security Essentials GSEC Practical, Version 1.3

April 2002

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

As a matter of policy, employees and contractors that perform work for the federal government are frequently asked to protect "sensitive" information. Recent terrorist events have raised the level of concern for sensitive information. The search engines of the Internet make it possible for anyone to pull together information from many sources. What was once seen as simply unclassified information may now be described as sensitive. The United States government has, over the years, put together many rules, laws, and directives that discuss the proper handling of Sensitive But Unclassified (SBU) information.

Information that is sensitive may or may not have a label such as SBU or "Eyes Only". For the person responsible for putting together a security policy, determining what information is sensitive and what may be published will be one of the most challenging aspects of the process. In this report, one will learn about the differences between classified and unclassified information. One will also learn about the many names by which sensitive information may be labeled. The history of the United States laws that affect the dissemination of sensitive information is addressed, and guidance is provided for identifying and protecting sensitive information.

Policy

As a portion of virtually every organization's policy, there will necessarily be rules and procedures that address the handling of information within that organization. Whether it is a corporation or a non-profit organization or the federal government, the loss of critical information can be damaging.

Information assurance, or information security, not only includes the methods for properly handling information, but also must include the methods for identifying potentially sensitive information. In many cases, information can be broken down into categories that identify its level of importance. The level of importance will often dictate the amount of time and money to be spent on protecting the data; the so-called risk management. An electronic funds transfer between banks would obviously have a high importance, whereas an email detailing the company picnic would have a low importance. Obviously the higher the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

importance, the greater the effort must be to protect that information.

When one is determining how to protect information, one must consider the following properties: confidentiality, availability, authenticity, and integrity. Confidentiality is the handling of information such that only appropriate persons shall have access. Availability is the characteristic that allows a piece of information to be accessible, even in the event of a disaster. Authenticity is the characteristic that provides assurance about the creator of a piece of information. Lastly, the integrity of information is a measure of whether it has been changed or modified up to and including the complete loss of the data.

The fact that the United States government classifies portions of its information for national security is well known. Less well known is the fact that many organizations working for the federal government must handle information considered sensitive, but unclassified. The policies for protecting and handling information that is classified are mostly well documented. Not so well documented are the policies and procedures for protecting data that is sensitive, but unclassified. The remainder of this report will focus on the history, identification, and handling of sensitive data.

History

The United States Constitution establishes that the United States government shall defend its citizens. After the Second World War, the National Security Act of 1947 was produced. Written during the tenure of President Truman, the National Security Act may be best known for the creation of the National Security Council and the Central Intelligence Agency (CIA). However, the National Security Act of 1947 and the Atomic Energy Act of 1954 were also key cornerstones to the current federal policies on classified and unclassified information.

Over the years, the federal government has frequently referred to some information as being “sensitive”. The Computer Security Act of 1987 states as a specific purpose:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

> "to require establishment of security plans by all operators of Federal computer systems that contain sensitive information;"[1]

The Computer Security Act of 1987 defines "sensitive information as follows:

> "the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy;"[2]

In other words, the information called "sensitive" in the Computer Security Act of 1987 is unclassified. Yet, the Act clearly states that organizations are responsible for protecting such data.

Perhaps more importantly, the Computer Security Act of 1987 establishes that the National Bureau of Standards is responsible for creating standards for the security of Automated Information Systems (AIS) within the federal government. In 1988, the National Bureau of Standards was renamed the National Institute of Standards and Technology, or NIST.

The Computer Security Act mentions the Privacy Act of 1974 so that information that would potentially harm an individual's right to privacy would also be considered "sensitive". Such information includes items like the individual's social security number or the details of a background investigation. The release of either of these pieces of information could be considered harmful to an individual's privacy.

Obviously, information that is "classified" will not fall into the SBU category. The Department of Defense clearly defines three levels of classification. As stated in the Department of Defense Regulation 5200.1-R (Information

---

[1] United States Congress, "Text of the Computer Security Act of 1987"
[2] United States Congress, "Text of the Computer Security Act of 1987"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Security Program), information may be classified as "Top Secret", "Secret", or "Confidential". These terms are further defined:

- "Top Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe."[3]
- "Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."[4]
- "Confidential shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."[5]

On the other side of the debate over information security are those individuals who want to have free and unconstrained access. Whether it is a journalist or simply a concerned citizen, the federal government made it clear that virtually all information not classified and not protected by the Privacy Act of 1974 should be made available to the public.

The Freedom of Information Act of 1966 made it mandatory for the executive branch of the United States government to release appropriate information upon request. The law allows for an individual to request information from a government agency under the Freedom of Information Act. The government must then evaluate the sensitivity of the information being requested. The government then releases the information in its entirety or after some sanitization has been accomplished.

[3] Department of Defense, "Information Security Program"
[4] Department of Defense, "Information Security Program"
[5] Department of Defense, "Information Security Program"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

However, the Freedom of Information Act was not quite that simple. For one, the federal government can classify information after receiving a request. In addition, the Freedom of Information Act lists nine exemptions that may be used to deny the release of all or part of the requested information. The first exemption deals specifically with classified information. The other eight exemptions may be used to deny requests for other reasons such as privacy issues or legal issues. If an item is determined to be exempt from the Freedom of Information Act, then the information contained therein could be considered Sensitive But Unclassified (SBU).

Sensitive But Unclassified (SBU)

The government often handles even unclassified data as sensitive data in order to provide as little intelligence to their adversaries as possible. For the most part, agencies use their own discretion about how to handle sensitive but unclassified data.

The Department of State Foreign Affairs Manual (12 FAM 541) states:

> "SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act."[6]

Note that it is the information that could harm an individual's privacy rights, or is otherwise exempt from the Freedom of Information Act, that will be considered SBU. At the web site parishioner.org, there is a link to "Diplomatic Cables". Upon reviewing the cable (i.e. message), it is clear that the Department of State marked almost every paragraph as "SBU". Please see the reference for "U.S. Embassy meetings on Heber Jentzsch".[7]

The Department of State used the term "Limited Official Use" or "LOU" until 1995. At that time, the Department of State ceased using LOU and began using "Sensitive But Unclassified". Also, SBU information is sometimes referred to as "sensitive unclassified information".

---

[6] Department of State, "12 FAM 540"
[7] Department of State, "Embassy Meetings on Heber Jentzsch"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Defense Security Service describes its definition of SBU in yet another way:

> "The term sensitive unclassified information as used here is an informal designation applicable to all those types and forms of information that, by law or regulation, require some form of protection but are outside the formal system for classifying national security information. As a general rule, all such information may be exempt from release to the public under the Freedom of Information Act."[8]

The Department of Defense uses yet another designation: "For Official Use Only" or "FOUO". The Department of Defense states that any document that contains "Department of State SBU information shall be marked as For Official Use Only".[9] In Department of Defense Directive 5200.1, it is stated that the "criteria for allowing access to SBU information are the same as those used for FOUO information."[10]

Similar Department of Energy labels include "Official Use Only" and "unclassified sensitive". The Department of Justice uses "Limited Official Use".

In many cases, the information that is considered sensitive but unclassified is not marked as such. Consider the story about a Chinese national attempting to gather information at an invitation only American Institute of Aeronautics and Astronautics (AIAA) and Ballistic Missile Defense Organization (BMDO) Technology Conference.[11] The uninvited guest attempted to gather brochures. He was found to not have any conference identification and was escorted from the conference.

The story illustrates two points. That information contained in company brochures could be considered "sensitive" by some authorities. And, adversaries of the United States government will gather potentially sensitive information contained in any source.

---

[8] Defense Security Service, "Protecting Sensitive Unclassified Information"
[9] Department of Defense, "Information Security Program"
[10] Department of Defense, "Information Security Program"
[11] National Counter Intelligence Executive, "Alert Employee Thwarts Overt Intelligence Collection Attempts"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Internet

In recent years, government departments and contracting companies have been reviewing the information made available through a variety of sources. The United States government has become increasingly aware of the potential sensitivity of information available via the Internet. Whether it is by the World Wide Web, or by FTP, information is flowing out of the government facilities and into the hands of the United States' adversaries.

Search engines connected to the Internet can rapidly display potential sources of information about whatever topic one might dream up. The fact that information from these independent sources can be collected and studied as a whole is of great concern to the United States government. Recent terrorist events caused such concern about a potential attack on nuclear power plants that many web sites were sanitized so as to make it more difficult for the United State's adversaries to find useful nuclear power plant information.

As the Internet grew during the 1990s, the federal government began revising its policies, laws, directives, and manuals.

Executive Order 12958 was issued on 17 April 1995 by then President Clinton. The executive order was titled "Classified National Security Information". As stated in the order, the purpose was to provide "a uniform system for classifying, safeguarding, and declassifying national security information".[12] While the order defined many terms that deal with typical Department of Defense classifications, the order did not specifically address SBU information. The order does provide a large amount of guidance on what may or may not be classified or declassified.

The Information Technology Management Reform Act of 1996, also known as the Clinger-Cohen Act,[13] assigns responsibility for ensuring adequate security measures on IT resources to each agency head. Obviously the head of each agency would not be performing the duties necessary to secure the information. What is important to note is that

[12] Defense Security Service, "Executive Order 12958"
[13] United States General Services Administration, "Clinger-Cohen Act of 1996"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the definition of adequate security could be different from one agency to another.

In 1995, the Secretary of the Department Of the Navy (DON) issued the instruction: SECNAV Instruction 5239.3. The subject of the instruction was the Information Security (INFOSEC) for the Navy. In section 7b of the instruction, "Fundamental INFOSEC Policy", the directive includes:

1. "Data processed, stored and transmitted by information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy."[14]

2. "The nature of the DON mission, accompanied by connectivity and data aggregation issues, has led to the determination that **all unclassified information processed by DON information systems is sensitive**. Therefore, all DON information systems shall be protected by the continuous employment of appropriate safeguards."[15]

3. "Classified information processed or stored by DON information systems shall be safeguarded as required by that level of classification."[16]

In the year 1997, the Computer Security Enhancement Act amended previous NIST responsibilities to include a broader range of goals and clients. In addition, the Act authorized NIST to help private industry establish standards for a non-federal Public Key Infrastructure. The Act also amended the Computer Security Act of 1987 to emphasize protection of "sensitive information" on systems "accessible through public networks".[17]

In 1999, the United States Army Corps of Engineers (USACE) issued a memorandum to all USACE commands. The memorandum's subject was "Protection of Transmitted Sensitive But Unclassified (SBU) Information".[18] The memorandum stated

[14] Secretary of the Navy, "SECNAVINST 5239.3"
[15] Secretary of the Navy, "SECNAVINST 5239.3"
[16] Secretary of the Navy, "SECNAVINST 5239.3"
[17] United States Congress, "Computer Security Enhancement Act of 1997"
[18] United States Army Corps of Engineers, "Protection of Sensitive But Unclassified Information"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

that SBU information must be protected whether it is marked as SBU or not. The memorandum also defined a wide range of possible SBU information, including contractual and financial information. The memorandum states that "National Security Agency (NSA) approved methods" for protecting SBU data must be used.

Individual Responsibilities

As the rules, laws, directives, regulations, and policies are written, individuals as well as their organizations are responsible for the security of information handled by Automated Information Systems within their control. Whether the individual is posting information about staff on the current project, or information about a bug encountered while writing a module for the project, the information could be determined to be sensitive.

It is apparent that most federal agencies have some definition of unclassified sensitive information. The decision about what information is sensitive is granted to various directors and department heads within these agencies.

One should be able to get approval for dissemination of information, in writing, signed by an official in the agency responsible for the information. Without such approval, the individual will at least partially accept responsibility for any harmful consequences of the information release.

Protecting the Information

As was suggested by many federal agencies, sensitive data must be protected for integrity, authenticity, availability, and confidentiality.

To protect information integrity, one has to preserve the information in its original state, or have a means of determining if the information has changed. One could save data to a backup media such as tape, and store the tape offsite to prevent corruption. For files or emails, one could use PGP signatures or generate hash codes; each could be used to verify the integrity of the file or email at a later date.

Authenticity of information is produced when one can guarantee the source of the information. PGP signatures can enable one to determine authenticity. Distributing the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

information on a media such as CD-ROMs, and perhaps including holographic images on the CD-ROMs, could enable one to verify authenticity as well.

Availability of information is best guaranteed with regular backups of the information, and redundant systems for serving the information to the clients. One might have a process continuously comparing the public web site with an internal web site to determine that the information is current and uncorrupted. Consider writing a complete and thorough disaster recovery plan that includes the names of those responsible for performing the work.

Confidentiality can be ensured with an appropriate set of authentication procedures or encryption of the data. Perhaps the data is sensitive enough to require two pieces of authentication such as a smart card and a password. Or perhaps the data is encrypted, and the private key is on a smart card. Some newer laptops are being sold with authentication hardware and encryption hardware so that all information on the device is unusable unless the owner authenticates with a thumb scan. Some systems even go so far as to encrypt the operating system.

Overall, the protection of all information will be a matter of risk management. The fact that some information may be sensitive but unclassified is not new. Rather, the concern increased as the information became easier to aggregate. One must balance the risk with the cost of protecting the information. Determine the information's classification, or sensitivity, first. Then determine what level of risk is acceptable. Finally search for the right fit of protective mechanisms and policies for the risk. Seek guidance from the officials whom ultimately own the information.

The National Institute of Standards and Technology has information that can help one evaluate security mechanisms and risk. The NIST's Information Technology Laboratory (ITL) is full of information to help evaluate and implement IT security solutions. NIST produces the Federal Information Processing Standards (FIPS), which are a result of the Computer Security Act. NIST also hosts the Computer Security Resource Center (CSRC), and makes available results from its Cryptographic Module Validation Program (CMVP). FIPS publications 140-1 and 140-2 define four security levels for cryptographic modules. The NIST Module

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Validation Program identifies the security level for each module evaluated.

The National Security Agency maintains information on its website concerning information security. The site has Security Recommendation Guides for the Microsoft Windows operating system, and the site has a security-enhanced version of Linux, including discussions and downloadable software.

The System Administration, Networking, and Security (SANS) Institute maintains a wealth of security related information as well. The SANS site and the Incidents.org site are both must reads for anyone attempting to determine the proper security policy for their IT infrastructure. If one can attend, SANS also offers training for everyone from the novice to the expert.

Summary

When producing the security policy for an organization, one must consider the potential sensitivity of all information. To be thorough, one must determine whether sensitive but unclassified information can be reasonably compartmentalized to reduce risk. Remember that the information may be considered sensitive even across internal divisions within the organization. The better compartmentalized the information is, the less likely the organization will be held liable for an improper release of information. A well-written policy, combined with well-trained staff, will help to ensure that such improper releases do not occur.

The Freedom of Information Act and the Privacy Act are both key to determining whether a piece of information is sensitive. However, these two pieces of legislation are not sufficient on their own to relieve an organization from all responsibility. The federal government has appointed appropriate agency heads as having the final decision on the protection of information within their organization. A non-federal organization will be expected to comply with the appropriate rules and regulations when its work is associated with any of the federal agencies.

When writing the policy or training the staff, be prepared to produce examples of the federal government’s codes and regulations that apply to the information within the organization. Sensitive information has a long history and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

it is fairly well documented. An organization is more likely to participate willingly with a new security policy if the history is well understood.

The chain is only as strong as its weakest link.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

1. Canter, Bryan, "Defense Message System" Automatic Digital Network is Dead – Long Live Defense Message System, 14 Aug 2001, http://www.gordon.army.mil/REGTMKTG/AC/SPR00/dms.htm
2. Defense Information Systems Agency, "IA Acronyms and Abbreviations", 3 Oct 2001, http://iase.disa.mil/acronym.html
3. Defense Logistics Agency, Technology Services and Infrastructure Support, "Home Page" PKI Infrastructure, http://www.dla.mil/j-6/cisdir/IApki.asp
4. Defense Security Service, "Executive Order 12958", 17 Apr 1995, http://www.dss.mil/seclib/eo12958.htm , 14 Nov 2001
5. Defense Security Service, "For Official Use Only" For Official Use Only (FOUO) and Similar Designations, 28 Nov 2001,

   http://www.dss.mil/search-dir/training/csg/security/S2unclas/Fouo.htm
6. Defense Security Service, "Protecting Sensitive Unclassified Information", 28 Nov 2001, http://www.dss.mil/search-dir/training/csg/security/S2unclas/Intro.htm
7. Department of Defense, "Defense Link News" Secret and Below Interoperability, 4 June 1998, http://www.defenselink.mil/news/Jun1998/t06051998_t604sasc.html
8. Department of Defense, "Information Security Program" DoD Directive 5200.1-R, Jan 1997, http://www.c3i.osd.mil/other/reg52001.html
9. Department of Defense, "Information Security Program" DoD Directive 5200.1-R, Jan 1997, http://www.dtic.mil/whs/directives/corres/pdf/52001r_0197/p52001r.pdf#xml=http://www.dtic.mil/search97/s97is.vts?action=View&VdkVgwKey=%2Fwhs%2Fhttpd%2Fwhs%2Fdirectives%2Fcorres%2Fpdf%2F52001r%5F0197%2Fp52001r%2Epdf&doctype=xml&Collection=whs&QueryZip=SBU&
10. Department of Defense, "Special Types of Unclassified Information Requiring Protection" DoD Directive 5200.1, 1997, http://www.c3i.osd.mil/other/5200_AP3.doc
11. Department of Energy, "DOE Directive G 241.1-1", 17 Aug 1998, http://www.directives.doe.gov/pdfs/doe/doetext/neword/241/g2411-1.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

12. Department of Energy, "DOE Proposes Draft Directive on 'Sensitive But Unclassified' Information", 18 Mar 1999, http://www.fas.org/sgp/news/doesbu.html

13. Department of the Navy, "Naval Policy" Sensitive But Unclassified (SBU), http://cpars.navy.mil/cparsfiles/sbu.htm

14. Department of State, "12 FAM 540" Sensitive But Unclassified (SBU) Information, 1 Oct 1999, http://www.foia.state.gov/masterdocs/12fam/12m0540.pdf

15. Department of State, "State Department Guidance on 'Sensitive But Unclassified'", 2 Feb 2000, http://www.fas.org/sgp/news/2000/02/sbu.html

16. Department of State, "U.S. Embassy meetings on Heber Jentzsch", http://parishioner.org/spain.html

17. Federal Aviation Administration, "http://www.faa.gov/ait/funcreq/chpt3.htm " Selecting Appropriate Mechanisms to Manage System Security, http://www.faa.gov/ait/funcreq/chpt3.htm

18. Idaho State University, "A Guideline on Office Automation Security", 5 December 1986, http://security.isu.edu/isl/ntmcp187.html

19. IEEE Computer Society, "GAO Reports DoD SBU Computer Security Inadequate",

    http://www.ieee-security.org/Cipher/Newsbriefs/1996/960522.GAOrept.html

20. International Trade Administration, "Pursuits Template" Administrivial Pursuits, 16 May 2001, http://www.ita.doc.gov/ooms/May_16.htm

21. Kasten Chase, "Contact Us" Kasten Chase Receives National Security Agency (NSA) Certification for Enterprise RASP, 2000, http://www.kastenchase.com/news/releases/pr010907NSAEnterprise.htm

22. National Archives and Records Administration, "Federal Register - Executive Order 12356", 2 Apr 1982, http://www.nara.gov/fedreg/codific/eos/e12356.html , 10 Dec 2001

23. National Archives and Records Administration, "The Constitution of the United States - Transcription", 31 Dec 2001, http://www.nara.gov/exhall/charters/constitution/constitution.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

24. National Counter Intelligence Executive, "NCIX – News and Developments" Alert Employee Thwarts Overt Intelligence Collection Attempts, Sep 2001, http://www.ncix.gov/news/2001/sep01.html

25. National Institute of Standards and Technology, "Computer Security Act of 1987", 11 Jun 1987, http://csrc.nist.gov/secplcy/csa_87.txt

26. National Institute of Standards and Technology, "Cryptographic Modules Validation Lists" FIPS 140-1 FIPS 140-2, 28 Mar 2002,

http://csrc.nist.gov/cryptval/140-1/1401val.htm

27. National Institute of Standards and Technology, "FIPS Home Page" Federal Information Processing Standards Publications, 1996, http://www.itl.nist.gov/fipspubs/index.htm , Nov 2001

28. National Institute of Standards and Technology, "FIPS By Category", 1995, http://www.itl.nist.gov/fipspubs/0-toc.htm

29. National Institute of Standards and Technology, "Untitled" Sensitive but Unclassified (SBU) Information Created, Processed, Stored, Or Transmitted In Electronic Format, 3 Feb 1997, http://csrc.nist.gov/fasp/FASPDocs/systemsec-plan/USAIDSecurityPlanBSPT5.htm

30. National Security Agency, "NSA Home Page", http://www.nsa.gov/

31. Oak Ridge Associated Universities, "Sensitive Unclassified Information", 12 Feb 1997, http://www.orau.gov/se/chpt4.htm

32. SANS Institute, "SANS Institute: Information Security Reading Room", http://rr.sans.org/index.php

33. SANS Institute, "Welcome to Incidents.org", 2001, http://www.incidents.org/

34. Secretary of the Navy, "SECNAVINST 5239.3" Department of the Navy Information Systems Security (INFOSEC) Program, 14 Jul 1995, http://www.fas.org/irp/doddir/navy/secnavinst/5239_3.htm

35. United States Army Corps of Engineers, "Protection of Sensitive But Unclassified Information", 21 May 1999, http://www.usace.army.mil/ci/impolicy/sbu.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

36. United States Army Corps of Engineers, "US Army Corps of Engineers Home", 25 March 2002, http://www.usace.army.mil/

37. United States Congress, "Computer Security Enhancement Act of 1997", 11 Nov 1996, http://www.house.gov/science/hr1903.html

38. United States Congress, "House Science Committee Approves Computer Security Enhancement Act", 1997, http://www.house.gov/science_democrats/archive/compsec.htm

39. United States Congress, "Text of the Computer Security Act of 1987 (Public Law 100-135)", 8 Jan 1988, http://www.house.gov/science_democrats/archive/compsec1.htm

40. United States General Accounting Office, "Information Security" Computer Attacks at Department of Defense Pose Increasing Risk, May 1996, http://www.gao.gov/archive/1996/ai96084.pdf

41. United States General Services Administration (GSA), "Clinger-Cohen Act of 1996" Information Technology Management Reform Act, 1996, http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/Clinger_CohenAct1996_4.doc

42. Wulf, Wm, "Cyber Security: Beyond the Maginot Line", 10 Oct 2001, http://www.house.gov/science/full/oct10/wulf.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: February 13th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced