Global Information Assurance Certification Paper

David_ Witherspoon_GSEC.doc
Certification and Assignment: GSEC Version 1.4b
Title of Paper: Local Security SOP

INTRODUCTION:

The following Local Security Policy Standard Operating Procedure has been drafted in support of an analysis team working within the Department of Defense. Some of the areas to be covered include: Markings, Safeguarding of Classified and Unclassified Documents; Marking, Safeguarding and Destruction of Tape Media; Internal Office Security to include Password Selections; Secure Communication; Use of Laptops for Emergency Contingency Plans; Checking the Security Containers and Completion of (Standard Form SF702); Completion of the Activity Security Checklist (Form 701) and Pretty Good Privacy. This initial Local Security Policy was purposely written by annex attachments so whenever another security problem is identified, the Security Policy can be easily revised or amended by adding another ANNEX.

HISTORY:

In thinking about what to write my paper on in conjunction with my GSEC study material, I found page 2-10A (Basic Security Policy) of the SANS GSEC Course; Subject: Identifying Security Policy particularly mesmerizing. Specifically where it stated the problem was "my organization doesn't seem to have a security policy" [1] from there a check was made of my work-related area and my workplace, indeed was in need of an internal security policy that would encompass our office personnel and personnel assigned on temporary duty for training. Safeguarding our current and archived data is of the utmost importance for its protection of this data. It can only be accomplished by astute concentration on physical security of our safes, rooms, etc, and the protection of information stored and accessed by our computerized assets.

Summary:

My paper is designed as a dual-purpose paper. It addresses the on-site need of the writer's work place for a Local Security Implementation Policy and to fulfill that need with a workable policy. It will hopefully give others thought of how they can improve their security environment in their respective work areas. The ANNEX 's attached is easily adaptable to fit other agencies/work places. Since security is a day to day practice, so much can be done to improve the security posture and reduce the threat. The information contained in the SANS Basic Security Policy was extremely helpful in the thought processes that aided in the development of this standard operating procedure. On the next page the SOP begins.

BASIC CERT SECURITY SOP

1. PURPOSE: The purpose of the CERT (Computer Emergency Response Team) Security SOP#1; Subject; as above, is to insure adherence to and conformity with established local procedures in accordance with Army Regulation 380-5 and Local Supplement to 380-5.

2. REFERENCES:

   a. AR 380-5 Department of the Army Information Security Program

   b. Local Information Security Program Plan.

3. SCOPE: This standard operating procedure applies to all personnel assigned or attached for duty with the xxx CERT at x x x x x x x x x x x x x x x x x x x x x x x x x x x. This includes military, civilian and contractor personnel.

4. RESPONSIBILITIES: The CERT Program Manager has overall responsibility for all security related matters as pertains to the CERT.

5. This SOP is broken down into the following Annexes for ease of use:

   a. Annex 1 - Marking and Safeguarding of Classified and Unclassified Documents

   b. Annex 2 - Marking, Safeguarding and Destruction of Tape Media

   c. Annex 3 - Internal Office Security

   d. Annex 4 - Secure Communications

   e. Annex 5 - Laptops for Emergency Contingency Plans

   f. Annex 6 - Checking the Security Container and Completion of SF 702

   g. Annex 7 - Completion of the Activity Security Checklist (Standard Form 701)

Synopsis of Annex 1

Within our CERT environment, we are required to handle Classified Documents and at times, to move/transport them from area to area. The documents include, but are not limited to SIPRnet messages; tasking orders, etc. It is of utmost importance that these messages/documents be handled in a manner that insures the integrity of their contents. All personnel working within the CERT, regardless of rank, title, or position, have a personal and individual responsibility for the proper safeguarding and protection of the information they have access to. This is particularly critical in the handling of Secret, Confidential and Unclassified Information. To this end the following Annex provides instructions for the proper marking of these documents.

ANNEX 1

MARKING AND SAFEGUARDING OF CLASSIFIED DOCUMENTS

1. Originators of classified information are responsible for:

   a. Marking their documents in accordance with Chapter IV AR 380-5 [2]

      (1). Sample Secret marked document at Incl 1 to Annex 1. (not Incl)

      (2). Sample Confidential marked document at Incl 2 to Annex 1. (not Incl)

   b. All file folders containing classified information will be stamped with the overall classification of the material found within; top and bottom, front and back.

2. Each person who has knowledge, control or possession of classified information is responsible for protecting that information at all times, no matter what its form may be, no matter how they obtained it.

3. Employees will store classified documents and media in approved security containers. Locked rooms, desks and file cabinets are not approved storage facilities. Employees will not store unclassified materials with classified materials unless the unclassified material supports the classified material. Also, employees will not store pilferable items and items having only monetary value such as cameras, cash, precious metals, jewelry, etc. in classified storage containers.

4. Combinations must be changed:

a. When the safe is put in use

b. Whenever an individual knowing the combination no longer requires access

c. When the combination has been subject to compromise

d. At least annually

5. The prime custodian (user) or one of the other custodians of the container will:

a. Complete SF 700, showing the names, addresses and phone numbers of the individuals who will have access to the storage facility and send it to the Security Office together with an informal memorandum addressed to the locksmith. The Chief Security Office or alternate will make arrangements for a trained technician to assist the custodian in changing the combination.

b. Set the combination under the supervision of a trained technician and record the combination on Part 2a SF 700. (A sample copy of SF 700 is attached as Incl 3 to Annex 1)

c. Attach Part 1, SF 700 to the inside of the locking drawer of the container, stamp Parts 2 and 2a to show the highest classification of information stored in the container, and take Parts 2 and 2a to the Security Office.

d. The Chief, Security Office or alternate will retain Parts 2 and 2a, Standard Form 700.

e. Custodians will safeguard and handle their combinations in the same manner as any other information of like classification. Only the custodians of a container may have access to the container's combination. If the custodian needs to record the combination, he/she will place it in a sealed envelope marked with the applicable classification, top and bottom, front and back. He/She will store it in a locked security container accessible only to the custodians of the container for which the combination is retained.

6. Opening and Closing Procedures for Security Containers:

a. Only custodians of the container, vault, or facility (those persons listed on the SF 700 or other access roster) may open and close the container. Custodians of classified storage containers and facilities will use SF 702, "Security Container Check Sheet" (A sample copy of SF 702 is attached as Incl 4 to Annex 1) to record all openings, closings and checks of security containers.

The custodians of the container or facility will post the SF 702 on the container or near the facility's exit (entrance).

(1) The custodian who opens the security container or facility will show the date and time, the container is opened on the SF 702 and initial the form in the "OPENED BY" column.

(2) The custodian who closes the security container will initial the form and show the closing time in the "CLOSED BY" column.

(3) The closer will have an appropriately cleared individual check the security container or facility at the end of the duty day. The checker will initial the

Synopsis for Annex 2

Within the CERT area, backups are a necessity. In addition to the retention of collected data for on-site use, forensics and investigational agencies commonly request specific blocks of data in relation to on-going cases. This data must be readily available; conspicuously marked as to classification and ready for dissemination upon official requests. Tapes must be stored in a climate control security container. Tape must be with date, level of backups and machine name. Tapes designated for destruction, will be handled thru the trash derby pickup. The following Annex addresses the markings, safeguarding and destruction of the tape media.

ANNEX 2

MARKING, SAFEGUARDING AND DESTRUCTION OF TAPE MEDIA

Each employee of the CERT is responsible for adhering to the following policies regarding Marking, Safeguarding and Destruction of Tape Media.

1. Tape backups must be marked with the applicable standard form label - in our case SF 710 (Unclassified Label for ADP media) in accordance with Paragraph 4-32 AR 380-5.

2. After a successful backup is completed, the tape will have the label attached and will have the level completed annotated on it, the date and machine name. The write ring should be moved to the protect position to avoid overwriting.

3. Blank tapes will be kept in a separate location away from the completed backup tapes.

4. Tapes that eventually become unserviceable will not just be thrown away. They must be boxed, taped and then coordination made with security for the trash derby pickup. The trash derby pickup conducted by security insures classified and sensitive media are properly disposed of. [8]

5. Due to the sensitivity of these backups in the CERT environment the completed backup tapes will be stored in the CERT security container.

ANNEX 3

INTERNAL OFFICE SECURITY

Each employee assigned to the CERT is responsible for adhering to the following Internal Office Procedures:

1. Password Selection (the don'ts)

   a. Don't use something you'd find in a dictionary

   b. Don't use a name [7]

   c. Don't use any variation of your personal or account name

   d. Don't use accessible information about you (such as phone number, license plate or SSN or anything to do with your environment. [4]

   e. Don't use a birthday [3]

   f. Don't use a simple pattern such as backwards, followed by a digit, or proceeded by a digit.

2. Password Selection (the do's)

   a. Use a mixture of upper and lower case letters as well as digits and punctuation.

   b. When choosing a new password, make sure it is unrelated to any previous password.

   c. Use long passwords (e.g. at least 8 characters long)

3. Password Selection (Protecting your Password)

   a. Don't write your password down anywhere or place it in an unencrypted file. Memorize it.

   b. Don't give or show your password, in particular to someone claiming to be from computer support or a vendor. [6]

   c. Don't let anyone watch you enter your password.

   d. Use the password for a limited time and change it periodically.

Method to choose Secure and Easy to Remember Passwords:

Choose a line or two from a song or poem, and use the first letter of each word. For example, “In Xanadu did Kubla Kahan a stately pleasure dome decree” “becomes “IXdKKaspdd.”

Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily Remember. Examples include “routboo”, “quadpop”., “and so on.

Choose two short words and concatenate them together with a punctuation character between them. For example: “dog;rain”, ‘book+mug”, “kid?goat”. [9]

Synopsis of Annex 4

Within our CERT environment, we deal with various Federal governmental and investigative agencies on a day to day basis. As such, exchanges of information pertaining to sensitive data taking place both verbally and thru the exchange of NIPRnet and SIPRnet e-mail. Due to the sensitive nature of the data transmitted, it is paramount that these transfers of data be encrypted and the encryption method utilized at Cert is PGP (Pretty Good Privacy). Additionally, we communicate orally on a daily basis with these agencies and with other integral operative areas that are necessary for the conduct of our business and for this, we use the STU (Secure Telephone Unit) phone. Instruction for implementation and usage of these two secure communications are as followings.

ANNEX 4

SECURE COMMUNICATIONS

Each employee of the CERT is responsible for adhering to the following policies regarding Secure Communications: [5]

1. Personnel will not discuss classified/sensitive information with agencies over normal non-secure phones. If necessary to discuss this type of information, a STU (e.g. the STU-III secure telephone unit) phone will be used to insure encrypted secure communication.

   a. Encrypted Phones will be posted with a warning that states "this telephone is subject to monitoring at all times; use of this phone constitutes consent to monitoring." The bottom portion of DD Form 2056 can be used for this purpose.

   b. Encrypted Phones will not be left unattended with the key in them. The CIK Key (crypto-ignition key) will be kept in the safe when not in use.

   c. To use Secure Phone:

      (1) Call agency you want to talk to before hand and see if they have a secure phone to get the number and say you'll call them right back on their secure line. [12]

      (2) Call number and say "going secure"

      (3) Turn CIK key to the right

(4) Push secure voice button

(5) Wait for the word secret to come up in the display area and the name of the organization you're talking to and then for the green light to go solid.

2. Personnel will not send clear-text messages of playbacks; raw data collections or TCP dumps over the internet unless the data has been encrypted thru the use of Pretty Good Privacy (PGP).

a. What is PGP?

PGP is a program that gives your electronic mail something that it otherwise doesn't have: Privacy. It does this by encrypting your mail so that nobody but the intended person can read it. When encrypted, the message looks like a meaningless jumble of random characters. PGP has proven itself quite capable of resisting even the most sophisticated forms of analysis aimed at reading the encrypted text.

PGP can also be used to apply a digital signature to a message without encrypting it. This is normally used in public postings where you don't want to hide what you are saying, but rather want to allow others to verify that the message actually came from you. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without the modification being detected by PGP.

b. Why should I encrypt my mail?

You should encrypt your e-mail for the same reason that you don't write all of your correspondence on the back of a post card. E-mail is actually far less secure than the postal system. With the post office, your mail is handled by postal workers. Take a look at the header area of any e-mail message that you receive and you will see that it has passed through a number of nodes on its way to you. Every one of these nodes presents the opportunity for snooping. [10]

c. What are public keys and private keys?

With conventional encryption schemes, keys must be exchanged with everyone you wish to talk to by some other secure method such as face to face meetings, or via a trusted courier. The problem is that you need a secure channel before you can establish a secure channel! With conventional encryption, either, the same key is used for both encryption and decryption or it is easy to convert either key to the other. With public key encryption, the encryption and decryption keys are different and it is impossible for anyone to

convert one to the other. Therefore, the encryption key can be made public knowledge, and posted in a database somewhere. Anyone wanting to send you a message would obtain your encryption key from this database or some other source and encrypt his message to you. This message can't be decrypted with the encryption key. Therefore nobody other than the intended receiver can decrypt the message. Even the person who encrypted it can not reverse the process. When you receive a message, you use your secret decryption key to decrypt the message. This secret key never leaves your computer. In fact, your secret key is itself encrypted to protect it from anyone snooping around your computer. [11]

Synopsis for Annex 5

In support of a 24/7 operation CERT analysts must be ready to operate from isolated locations due to snowstorms, floods electrical outages and other designated situations. In order to have logistical control over computer assets belonging to the CERT, the following procedures that are contained in Annex 5 apply.

ANNEX 5

LAPTOPS

Each employee of the CERT is responsible for adhering to the following policies regarding laptops:

1. In case of inclement weather or other emergencies our contingency plan involves the issue of laptop computers to the analysts of the CERT for use at designated locations.

   a. Employee must insure upon issuance of the Laptop that they have a current Optional Form 7 (Property Pass) filled out correctly authorizing them to transport the laptop off post and back again.

   b. Employees will not leave the laptop in the vehicle for an extended period of time. Laptop should be under employee constant supervision. While working at designated location employee should insure unauthorized personnel do not have access to the laptop or what is on the screen while work is being accomplished.

2. Laptops when issued for contingency purposes are to be utilized for official business only in support of the CERT operation.

Synopsis for Annex 6

All Classified documents must be secured in a security container when not in use. To insure an account trail of the documents, the following procedure will be utilized for opening, closing and checking of the security container.

ANNEX 6

CHECKING THE SECURITY CONTAINER AND COMPLETION OF SF 702 "SECURITY CONTAINER CHECK SHEET"

1. Checking the security container:

   a. Verify all drawers are closed and ensure latch is in the closed position.

   b. Spin the combination dial in a clockwise direction to ensure that lock has engaged and the dial spins freely. Turn the dial slowly for the first time in case the lock was left in the open position. Once you have verified the security container is locked then the combination dial should spin freely in both directions.

   c. Attempt to operate the latch and to open all drawers to verify they are locked in the closed position.

2. Completion of the SF 702 (Security Container Check Sheet)

   a. The custodian (or user) of the security container will write the container number and its location at the top of the SF 702 and note month and year in the space provided.

   b. Each opening and closing will be recorded.

   c. The custodian or user will note non-duty days, by writing NONDUTY DAYS on the appropriate line on the SF 702 next to the appropriate date.

   d. If the custodian or user opens the container after normal duty hours, he will write NONDUTY HOURS across the SF 702 next to the appropriate date before completing the OPENED BY column.

   e. An individual other then the person who closes the container will check the Security container at the end of the day and insure it is locked. In the CERT case this has been designated to third shift and should be completed by 0800 each morning. The checker will complete the CHECKED BY column to, certify completion of the check.

f. If the custodian (user) does not open the container on a given day the checker will write NOT OPENED next to the appropriate date and complete the CHECKED BY column.

Synopsis for Annex 7

The activity Security checklist is a five question checklist that must be noted by the last person out of the office. This check sheet is marked 1 thru 31 for each day of the month. Questions are as follows:

a. Have the Security Containers been locked and checked?

b. Are desks, wastebaskets and other surfaces and receptacles free of classified materials?

c. Are windows and doors locked?

d. Are typewriter ribbon and ADP devices (e.g., Disks, Tapes) stored in a Secret Container?

e. Has the Security alarm been activated?

ANNEX 7

ACTIVITY SECURITY CHECKLIST (STANDARD FORM 701)

1. These checks should be performed whenever possible by someone other than the person who performed the Security Container Checks.

2. For each of the five types of checks listed, perform the activities associated with that check and signify completion by entering a checkmark in the Appropriate block under the date the check was completed or "N/A" where not applicable (for the CERT at xxx, currently row 5 is "N/A").
   In the CERT this check will normally be performed at approximately 08:00 EST every day except 08:00 EST Sunday. The person performing the Activity Security Checks at 08:00 Monday will annotate the Sunday check by writing "NON-DUTY DAY" in that column if it has not been completed by someone performing the checks over the weekend.

3. The person on 08:00 Saturday will call one of the operations staff in Bldg xxx Rm xx at 3-xxxx to conduct the security container check at 08:00 Saturday if the analyst is working alone on that shift.

CONCLUSION:

Our CERT staff is the most cost-effective security countermeasure. They are generally the first to be impacted by potential security incidents and their compliance with security policy can make or break a security program. A staff that is aware of security problems, can prevent incidents and mitigate damage when incidents occur. Given the importance of the staff as a security control, awareness is therefore the most important part of an organization's security program. The threat is everywhere, from the transmission of e-mail messages to the data we store in our computers.

By having a comprehensive adoptable Local Security Policy in place, our CERT personnel are increasingly aware, that there are security dangers residing each day in the area in which we work. Before this standard operating procedure was written, the writer of the paper performed an internal risk assessment within the immediate work area and upon completion of that assessment, formulated a standardized Local Security SOP. This Standard Operating Procedure is consistent with higher level guidance and is current and readily available to all employees.

In conclusion, as this paper is read, hopefully it will cause other activities, agencies, and personnel to think about their local area and determine their threshold of vulnerability.

Resources

[1] Kramer, Carol; Northcutt, Stephen; Kirby, Fred "Basic Security Policy" Sans GIAC 2001 (Page 2-10A)

[2] US Army AR 380-5 "Department of The Army Information Security Program"
URL: HTTP://www.army.mil/usapa/epubs/Pdf/r380_5.pdf

[3] Garfinkel, Simson, Spafford, Gene "Practical Unix and Internet Security" O' Reilly. & Associates 1996 (Page 64)

[4] McClure, Stuart; Scambray, Joel; Kurtz, George.
Hacking exposed (Network Security Secrets and Solutions).
Berkeley: Osborne/Mcgraw-Hill, 1999 (Page 462)

[5] Department of Defense Security Institute "STU-III Handbook for Industry" 1997
URL:HTTP://www.Tscm.com/STUIIIhandbook.html

[6] San Jour, Joe; Arensburger Andrew; Brink, Anne "Choosing A Good Password" 1999
URL:HTTP://www.cs.Umd.edu/faq/Passwords.shtml

[7] CERN Security Handbooks "Practical Compute Security for CERN users
URL:HTTP://www.consult.cern.ch/writeup/sercurity/security_3.html#SEC7

[8] Integrated Publishing "Magnetic Tape and Diskette Destruction"
URL: HTTP://www.infodotinc.com/incs/34.htm/

[9] Advanced Laboratory Workstation System “Selecting good Passwords
URL:HTTP://www.alw.nih.gov/Security/Docs/passwd.html

[10] Chapter 1. General questions and introduction
URL: HTTP://www.pgp.net/pgpnet/pgp-faq/pgp-faq-general-questions.html#pgp-what

[11] Encryption FAQ's
URL: HTTP://www.evadenet.com/faq/encryption.shtml

[12] STU III (Secure Telephone and KSD-64)
URL: http://webhome.idirect.com/~jproc/crypto/stuiii.html