Administrative Inquiry (AI) Guidelines for Information Systems (IS)

Guidelines for Conducting an AI Involving a Nonaccredited IS

The format of the information is NOT important. Classified information, whether in text, binary, pixel, or other formats, is still classified.

It might be helpful to establish an emergency team and develop a contingency plan in the event that there is a security violation involving a nonaccredited IS. As a minimum the team should consist of people with hardware, software, and security expertise. If no security expertise is available, be sure also to follow the attached guidelines for the Security Representative. The team should follow the guidelines below:

For multi-user systems, depending on the suspected severity and magnitude of the problem, consider (1) stopping all remote (dial-up) processes, and (2) stopping all local user processes. (In some operating systems such as VMS, processes may be suspended until corrective actions are completed. This will protect innocent users from losing work performed up to that time.) Some situations may not warrant stopping all local user processes (e.g., having one classified number in electronic mail limited to a few terminals and the information was immediately deleted).

It is a good idea to document steps taken and when. This will assist in writing your Administrative Inquiry (AI) and provide concrete evidence of your corrective action.

Consider having a second individual observe the procedures. This helps for verification and ensures no steps are missed.

It is best to contact your DSS computer specialist when the problem arises to ensure that plans for your corrective action are adequate. Many times companies believe they have taken appropriate action only to find out two weeks later that they did not properly declassify the system.

In cases where a classified file is found on a system and you are not sure who placed it there, it is not a good idea to erase the file immediately. Rather, take precautions to identify the file name, creation/modification date, owner, and protection code. This can be done on some systems using an automated audit trail. Temporarily protect the file to the highest privilege level.

To determine the extent of the compromise and gain a better understanding of how the particular system works, use the attached guidelines for interviewing both users and system support personnel.

Once the extent of the compromise has been determined and the exact locations of the information on the system are known, begin declassification procedures. Follow the National Security Agency (NSA) guidelines for declassification of each piece of equipment and media. If overwriting is your selected method, DO NOT JUST WIPE THE FREE SPACE ON THE DISK as clipboard/buffering/temporary working files may be overlooked. Be sure to perform a verification following the overwrite

procedure to ensure it worked properly. A declassification/destruction record is appropriate.

Additional Note: In situations where the system is approved, located in a closed area, and the door is inadvertently left open, some portions of this guide may also apply. Be sure to check any automated audit trails in place to ensure no unauthorized person accessed the system. If the system is simply a remote terminal with a printer and is on-line to a user agency, be sure to contact the user agency for assistance. Consider things such as who could have been on the system during that period and was there any classified output that could have been removed. Most user agencies in those instances are running automated audit trails and can help with the AI.

Security Representative Responsibilities During an IS AI

Read guidance in Paragraph 1-303, NISPOM, and call your DSS computer specialist.

Ensure as much declassification and clean-up as possible is performed quickly (i.e., laser printers cleared, PCs powered down, printer ribbons, hardcopy output, and other media stored immediately).

Station an appropriately cleared individual with the equipment that cannot be declassified immediately (i.e., internal fixed disks). DO NOT LEAVE ANY equipment UNATTENDED that has not been properly declassified.

If you are not knowledgeable of the system, have someone who is knowledgeable with you when you interview users and system support personnel. This will ensure that all aspects of the technical issues are addressed.

After you have interviewed system support personnel and have determined which operating systems are applicable, try to locate within your company overwrite programs which would be authorized if the systems were approved (i.e., Norton Utilities, Disk Express 1.5, Sun's Purge, etc.). If they are not available, contact your DSS computer specialist or someone you know who has the programs.

Carefully document events, corrective action, and declassification. Submit a preliminary report immediately, followed by a final report within 15 days.

Questions for System Support Personnel During an Administrative Inquiry

KEY: Where is the information now located, and what was the flow of information within the system to reach its ultimate destination?

Is the system either clustered or networked? (On what other systems is the information potentially located?)

What operating systems are run in conjunction with the system(s)?

On what disk is the classified information now located?

Is there a common disk "farm"?

Does the system have disk mirroring or disk shadowing capability (two disks)?

Are there swap spaces, paging files, core or crash files?

Are there other buffering files such as print spoolers? If so, was the file actually transferred to the spooler or did the spooler only retain information as to where the file is located?

Are there any other buffers?

Was there uploading/downloading of files to other attached systems such as PCs or workstations?

Do the system, database, or other applications/programs do backups at regular intervals (e.g., every 20 minutes)?

Have system backups been made since the information was placed on the system?

Was the information deleted prior to backups being performed? If so, was it deleted or was delete/erase used? Does the delete/erase in VMS perform a one-time overwrite?

If backups were performed, what type of backup was done? Was it an incremental backup (which only updates files), or was it an image-type of backup (which captures deleted files)?

Can the backup tape containing the classified file be isolated?

What specific types of media were involved? (Use this as an inventory to ensure that EACH type of media is properly declassified.)

a. Tape with a coercivity of less than 350 oersteds?

b. Tape with a coercivity between 351 and 750 oersteds?

c. High-energy tape with coercivity of over 750 oersteds?

d. Floppy or Bernoulli disks?

e. Internal or external disks (rigid media)?

f. Non-volatile memory that can potentially contain classified material?

Has maintenance, including remote diagnostics, been performed which could have copied or further compromised the information?

Is there anything else that should be considered?

Other questions, as appropriate.

Questions for Users During IS AI

What information did you place on the system?

How many files were created?

When (date and time) was the file created?

What was the file name?

Is the file known by another file name?

Has the file ever been combined or merged into another file or data structure?

Has the file been compiled?

Have you transferred the file (or any other file as mentioned above) to other disks or media?

Is the file shared? If so, with whom?

Who else has your password?

Did you produce any hardcopy output?

a. If so, where is it now?

b. What did you do with the ribbon?

c. Did you do anything to clear the printer?

Ask any other questions, as appropriate.