NSTISSAM INFOSEC /1-99
July 1999

THE INSIDER THREAT

TO

U. S. GOVERNMENT

INFORMATION SYSTEMS

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7/1/1999	Report 7/1/1999

4. TITLE AND SUBTITLE
The Insider Threat to U.S. Government Information Systems (NSTISSAM INFOSEC/1-99)

5. FUNDING NUMBERS

6. AUTHOR(S)
Hayden, Michael

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Security Agency
9800 Savage Road, Suite 6716, Ft. Meade, MD 20755-6716

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This NSTISSAM focuses on the insider and the potential damage that such an individual could cause when targeting today's IS. It points out the various weaknesses (vulnerabilities) in today's IS an insider might exploit and highlights approaches to solving these problems. In taking corrective action, it is necessary to consider technical and procudural steps in deterring the insider. Finally, we propose, in priority order, recommendations that mitigate the threat posed by the insider. Our approach is not to provide an exhaustive list, but rather offer recommendations that could have the greatest immediate return against this serious threat

14. SUBJECT TERMS
IATAC Collection, information security, insider threat, vulnerabilities, insider abuse

15. NUMBER OF PAGES
46

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

UNCLASSIFIED

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. Today's Information Systems (IS) provide enormous leverage and access to vast amounts of sensitive, unclassified, and classified mission critical data. The potential for abuse is obvious.

2. This NSTISSAM focuses on the insider and the potential damage that such an individual could cause when targeting today's IS. It points out the various weaknesses (vulnerabilities) in today's IS an insider might exploit and highlights approaches to solving these problems. In taking corrective action, it is necessary to consider technical and procedural steps in deterring the insider. Finally, we propose, in priority order, recommendations that mitigate the threat posed by the insider. Our approach is not to provide an exhaustive list, but rather offer recommendations that could have the greatest immediate return against this serious threat.

3. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from the Secretariat at the address listed below.

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat (I42) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 • UFAX: (410) 854-6814

UNCLASSIFIED

ADVISORY MEMORANDUM ON THE INSIDER THREAT TO U. S. GOVERNMENT INFORMATION SYSTEMS (IS)

I. INTRODUCTION

The February 28, 1994 Joint Security Commission report to the Secretary of Defense and the Director of Central Intelligence entitled "Redefining Security" recognized the insider threat problem. It found that:

"The great majority of past compromises have involved insider, cleared persons with authorized access who could circumvent physical security barrier, not outsiders breaking into secure areas."

For this reason, the Commission highlighted two areas for particular attention. First, personnel security lies at the very heart of our security system, and the trustworthiness of those who deal with sensitive and classified information must be ensured. Second, Information Systems (IS) security requires increased attention. U. S. Government organizations are increasingly dependent on IS in performing their complex missions. The evolution of IS technology is, however, much faster than that of IS security technology. Overcoming this problem will require careful threat assessments, investment strategies, funding, and management attention if we are to protect the integrity, availability, and confidentiality of our information assets. These themes, emphasized by the Commission, continue to be vital in solving the insider problem and are reflected in this advisory.

II. THREAT TO U.S. GOVERNMENT INFORMATION SYSTEMS FROM INSIDERS

While government IS face a variety of threats from a variety of sources, the greatest potential threat comes from insiders with legitimate access to those systems. Data is sketchy on the extent of insider abuse of IS in general, and also of insider abuse of government systems. It is likely that most government insider abuse incidents are not reported beyond the parent organization and are dealt with internally; there is no central repository of government insider computer incident investigations.[1]

[1] For perspectives on the insider threat to the private sector see “The Insider Threat to Information Systems: A Framework

The 1998 “Computer Crime and Security Survey" conducted by the Computer Security Institute and the FBI International Computer Crime Squad's San Francisco office provides data from 520 security practitioners in U.S. corporations, government agencies, financial institutions, and universities. Government agencies were not identified nor was it reported what percentage of the total responses their information comprised. Of those reporting they had experienced unauthorized use of their computer systems in the previous year, 36 percent said they had experienced such incidents from inside their organization. Overall, 89 percent identified disgruntled employees as the likely source of attack, and 39 percent said insider abuse had cost the parent organization financial loss.

Insiders can be employees, contractors, service providers, or anyone with legitimate access to a system. All insiders have some degree of physical or administrative access to IS. The greater the individual's knowledge of and access to the system, the greater the potential threat from that person, with individuals having privileged access posing the greatest potential threat.

Using System Administrator (SA)-assigned or surreptitiously acquired computer access privileges, insiders have the capability to compromise, modify, or destroy information stored on the system, as well as the ability to inhibit its access to others. The insider is often self-motivated, knows the security of the system, and raises no alarm by his/her presence. For these reasons, if insiders volunteer their services to, or are recruited by, a foreign intelligence service, they can provide not only systems output such as printouts or magnetic media, but also specific information about the system. Insiders can also be co-opted or coerced to assist terrorists, drug traffickers, or other criminal elements or may be sympathetic to the goals of any of a broad array of nonstate actors.

IS are accessible at various lifecycle points from design, through production, test and evaluation, shipping, operations, and maintenance. Further, the modern trend of outsourcing and the use of Commercial-Off-The-Shelf (COTS) products have dramatically expanded the pool of insiders, giving third parties access to hardware and software at many lifecycle points.

1. Insider Categories

Some computer investigators have cited four categories of the insider problem: traitor, zealot, browser, and well intentioned. The traitor category includes persons who have a malevolent intent to damage, destroy, or sell out their organization.

The zealot category involves an insider who believes strongly in the correctness of one position or feels the organization is not on the right side of a certain

---

for Understand and Managing the Insider Threat in Today’s Business Environment,” An NSIE Workshop, June 18, 1998.

issue. In this case, the insider may try to "correct the organization." The method of correction may involve unauthorized disclosure of information, destruction of databases, or providing access to outsiders or other unauthorized insiders.

The browser category consists of persons who are overly curious in nature (often a violation of the need-to-know principle), while the well-intentioned insider commits violations through ignorance. Downloading shareware, disabling virus protection software, using unapproved CDs can all provide the assistance a hacker needs to penetrate a system. The well-intentioned user becomes the unwitting associate. Much work remains to be done to better profile the government insider computer abuser.

2. Insider Examples

In 1988, a Libyan intelligence agent obtained names, addresses, and home phone numbers of more than 1,000 federal employees at U.S. military and intelligence agencies. The information was obtained from his wife, who had access to the Metropolitan Washington Council of Governments listing for carpooling purposes through her job as a computer operator with the Virginia Department of Transportation. This was information that could have been used to assist in a terrorist operation.

Also in 1988, two Israelis associated with Israel's nuclear-weapons program illegally accessed a supercomputer at the Los Alamos National Laboratory's nuclear weapons facility in New Mexico. Congressional investigators reported that the Israelis used a friendly lab technician's access code and personal computer to connect into an unclassified but highly sophisticated Cray computer to work on designs for a nuclear-weapon detonator. The Israelis left the country before the intrusion was detected, and the technician was disciplined.

Drug dealers have used Department of Motor Vehicles (DMV) databases to check the registration of potential customers' automobiles. If the auto was not registered, the dealers assumed the individual was a law enforcement officer. One dealer was an Operations Specialist at the California Department of Justice. He used his authorized access to the Justice Department's Law Enforcement Data Center to query the DMV database.

In 1993, the General Accounting Office (GAO) determined that insiders posed the greatest security threat to the National Crime Information Center (NCIC). GAO cited 56 examples of intentional insider misuse of NCIC. Most of this misuse was relatively benign use of information for personal purposes (determining whether friends or relatives had criminal information), for profit (selling it to private investigators who were conducting background investigations on applicants for employment), or for political gain. In some cases, the misuse of NCIC information jeopardized the safety of citizens and potentially of law enforcement personnel. The most extreme example involved a former law enforcement officer who obtained NCIC information from three other officers and used it to track down his girlfriend and murder her. In another case, an NCIC terminal operator conducted background searches for her boyfriend, who was a drug dealer. He asked her to check the criminal history records of new clients to determine if they were undercover drug agents. She continued her activity until supervisors detected an unusual number of inquiries from her terminal.

According to a report of the Internal Revenue Service (IRS), as of 1993, 369 employees of the IRS's Southeast Region had been investigated or disciplined for using government computers to create fraudulent tax refunds or to browse through tax records of friends, relatives, neighbors and celebrities. One employee had altered approximately 200 accounts to receive kickbacks from bogus refund checks. Upon receipt of the report, Senator Glenn, Chairman of the Senate Governmental Affairs Committee, recommended that the investigation be extended beyond the Southeast Region.

More recent government insider abuse of IS was reported in September 1998. Social Security Administration (SSA) officials revealed how SSA accomplices assisted a West African credit card fraud ring by looking up records of credit card customers and providing the West Africans with additional identifying information to activate those cards. Twelve SSA employees and three contract security guards are allegedly involved in selling the information for $10 to $50 per record. SSA officials believe that files on approximately 20,000 people have been accessed in this manner.

In July 1997, a former U.S. Coast Guard employee used her programming skills to access the service's nationwide personnel database and deleted crucial data that caused the computer system to crash. The crash wiped out almost two weeks' worth of personnel data used to determine promotions, transfers, assignments, and disability claim reviews. It took 115 Coast Guard employees working more than 1,800 hours to recover and reenter the data, at a cost of more than $40,000. The employee reportedly felt her attempts to report improper and illegal conduct by a computer contractor were not taken seriously enough. She subsequently filed an EEO complaint, alleging a hostile work environment and resigned her job. According to the FBI, the precision of the hacking indicated it was done by someone with inside knowledge.

III. VULNERABILITIES

3. General User Access

Whereas threat focuses on the intent and, capabilities of insiders to do harm, a vulnerability is a characteristic or weakness of IS (e.g., system security procedures, hardware design, internal controls, etc.) that insiders can exploit. The examples in the previous section showed that the vulnerability most widely and easily exploited by an insider was the lack, or ineffectiveness, of controls and checks to prevent the insider from removing sensitive documents, computers or computer output media from their work areas. The vulnerability has increased over the past 10 years as organizations have relaxed exit checks and restrictions in response to an easing of Cold

War tensions, declining resources, and increased employee use of portable and home computers.

The vulnerability of an insider simply removing sensitive or classified information from work is further compounded by the ever-expanding access a typical

employee has to information as a result of increased networking. The connectivity may even be greater than is generally known because configuration control of networks is often lacking. In general, most U.S. Government employees with legitimate access to government systems and networks can browse and download information from several systems and networks. Use of applications and graphics packages provide them with additional privileges such as read and write capabilities. Employees, depending on their job function, may have the ability to modify, manipulate, and delete data they have access to, or they may be able to download or upload information regardless of its sensitivity. Besides copying and physically removing information, an insider could also copy the information into an e-mail file and send it, undetectable by human review, to themselves or someone else over the Internet from their office.

4. Privileged Access

Access is greater for certain employees at various points in the lifecycle of a U.S. Government system, and as a consequence, these employees have the ability to do more than just compromise information from the system. System programmers, for example, by virtue of their role in the design, production, testing, and evaluation of a system, can introduce malicious code, such as viruses, time bombs, or Trojan Horses, that could result in severe denial or disruption of service problems at predetermined times. They could also put in backdoors for exfiltrating information. It should be noted that the incorporation of commercial vendors into the government arena will increase the risk.

U .S. Government systems are especially vulnerable to insiders who have authorized root access privileges, such as system administrators. An insider with system administrator privileges could make subtle and undetectable changes to files, data, and access permissions. They could also make more obvious, detectable changes such as denying user access or taking over control of the entire system/network. Specific denial of service attacks could include shutting down routers, closing access to ports to disable dial-in capability, deleting network files so connectivity cannot be established, and renaming the server so other machines do not recognize it.

5. Unauthorized Access

Much like an outside hacker, an insider with authorized access to some systems could execute various attacks to gain unauthorized access to other systems or deny service to users of these other systems. An insider could manipulate files that facilitate the provision of services on virtual/remote machines. Common attacks of this type are directed at hosts and network file servers that facilitate workstations sharing files and services across an enterprise network. Another attack of this type exploits weaknesses in protocols to spoof users or reroute traffic. Examples include spoofing Domain Name Servers to gain unauthorized remote login, and bombing, that uses Internet Control Message Protocol (ICMP) to knock a machine off the air. Other well known attacks include source routing to indicate a trusted host source and Transmission Control Protocol (TCP) sequence number guessing to gain access and hi-jack a legitimate connection. Bombing a router to knock it off the network, flooding the network with garbage packets, and flooding mail hubs with junk mail are just a few of the alternatives insiders have to deny service.

System administrators, operators, or programmers with software knowledge could exploit vulnerabilities in software that runs with system privileges. Well known attacks involve sendmail and X-Windows server vulnerabilities. Recently, there has been a proliferation of alerts regarding operating system vulnerabilities. New vulnerabilities are discovered for various software and hardware platforms almost daily, vulnerabilities, and patches are reported through the various computer emergency response alerts and bulletins. Privileged insiders are the primary recipients of these alerts and bulletins.

6. Insider-Facilitated Outside Access

To reduce their risk of detection, insiders could do nothing more than facilitate outside access or attack.. Insiders could, for example, introduce viruses into systems by placing contaminated disks into the systems or downloading contaminated Internet attachments such as well known PostScript, Active-X, and MS Word macro viruses. They could provide an open door to the destructive outsider through the Internet or create a covert channel to signal private information outside the virtual private network.

The release of the Trojan, Back Orifice, in August 1998 has added a new dimension to the well-intentioned insider threat. Many computer users, believing they were helping their security personnel identify and eradicate this risk, downloaded programs purported to find and eliminate Back Orifice. The most widely known, Bo Sniffer, was actually a trojan in itself. Instead of eradicating Back Orifice, it ensured the program was loaded and set fully functional, allowing at will access to systems by an attacker.

7. Dependency on Commercial Networks

The government operates numerous networks. These networks may start as private networks, go through leased or public networks and terminate as private networks (e.g., SECRET Internet Protocol Router Network (SIPRNET). Approximately 90 percent of U.S. Government telecommunications services traverse public/commercial networks at some point, primarily the Internet and the Public Switched Telephone Network., but also cellular and satellite networks. Access is gained typically through service providers. The Federal Government has structured a number of network service contracts that procure network services for government use. These include the Federal Wireless service and FTS 2000 and are provided by public network providers.

The Public Switched Network is vulnerable to information compromise, denial or disruption of service, and unauthorized modification of network databases/services. Other potential vulnerabilities include the use of switched versus

dedicated lines, making availability a concern; the ability of an insider to cut a cable, thus denying, delaying, or interrupting service; and the possibility of a network administrator entering the wrong Internet Protocol address to reroute information to an adversary.

8. Physical Access

Lack of more stringent physical access controls affords the insider the opportunity to access facilities and highly sensitive, or classified areas within those facilities, such as computer rooms, network centers, and sensitive compartmented information facilities. Many users, especially system administrators and computer operators, have authorized physical access to computer rooms housing servers, modem pools, router boxes, and other equipment from which they could physically adjust settings, steal equipment with sensitive information or disable equipment. An insider familiar with the facility, in conjunction with loose controls and the use of social engineering techniques, might also be able to use this inside knowledge to gain physical access to areas outside of their approved level of access.

9. Data Aggregation

Data aggregation can be described as the collection and reassembly of pieces of information (or parts of several databases) to provide details that differ from the original purpose of the information or databases. Additionally, it may include the use of data contained in a database, but sorted differently than originally envisioned. The results obtained from recombining or recompiling data are not only different from the original intent, but are designed to satisfy the varying needs of the person or organization doing it. Insiders have a unique advantage in that they have access to the original data, often have the capability and knowledge to sort it differently to satisfy different purposes and/or can modify the original data. Insiders also have access to unclassified databases that are not accessible to the public. Providing this information to a requestor or modifying it could prove detrimental to the original owner of the data. Often it is possible to deduce classified information from these unclassified, but restricted or proprietary databases. The insider is often in a better position to access these databases or has the knowledge to manipulate them without being detected.

10. Homepages

With the proliferation of "net" homepages, another vulnerability becomes available to the insider. Whether dealing with Internet or intranet homepages, and whether these pages are official or personal in nature, a common tendency is for much of this information to spill over onto other sites. The lines between "official" information and "personal" information are often fuzzy, causing computer-savvy employees to post data that might be highly sensitive. A malicious insider (or even an innocent) could

easily compile and deposit information that would give an adversary a distinct advantage in ascertaining friendly capabilities, strengths, and weaknesses.

For example, during recent Operations Security (OPSEC) surveys, concern was expressed over personal homepages that had been created by members of the U.S. military. Some personnel were putting unclassified work-related information on their personal homepage. Some sites contained data that directly pertained to missions (e.g., timing, locations) while others dealt with personalities and units involved.

Other homepages have been observed to contain information about the system they are on, the IP address, and names and phone numbers of associated personnel. Many homepages also contain hot links to other sites. While this is advantageous for the organization, it also provides information to anyone else reading the homepage. Who you are associated with and with whom you frequently do business or access information from can provide good insight into an organization and its operations. Homepages must be looked at in terms of "what are we giving away?" as well as "what do I need to put on it?" Even though much of the data might be accessible to an outsider, the insider holds an enviable position, commanding a wide-angle viewpoint of what information is available, as well as its significance to the organization. Considering that even adversaries do not have unlimited resources, anything that can focus the collection effort is extremely useful.

A related problem concerns unclassified message traffic sent organization-wide that details positions, names, phone numbers, e-mail addresses, server IP addresses, and a host of other information. While a few people need this complete listing, not everyone does. Messages of this type provide excellent database material and starting points for adversaries.

On 24 September 1998, Deputy Secretary of Defense John Hamre issued a memorandum ordering the following information be immediately removed from publicly available DoD World Wide Web (WWW) sites:

a. Plans or lessons learned that would reveal sensitive military operations, exercises, or vulnerabilities.

b. Any information that would reveal movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

c. All personal information in the following categories about U.S. citizens, DoD employees and military personnel:

(1) Social Security Numbers
(2) Dates of Birth
(3) Home Addresses
(4) Telephone numbers, other than numbers of duty officers that are appropriately made available to the general public.

d. Names, location and any other identifying information about family members of DoD employees and military personnel. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASDC3I) was to develop policy and procedural guidelines to address operational, public affairs, acquisition, technology, privacy, legal and security issues associated with the use of DoD WWW sites.

IV. PERSPECTIVE FROM NO-NOTICE EXERCISES

It should come as no surprise that the three most important considerations in IS security are: access, access, and access. Most access is granted to cleared personnel, who are then treated as trusted users. However, it is possible that an outsider can obtain access by breaking into a system and thus assume trusted user status. Once on the inside, with trusted user status, it is possible that a real outsider has access to the full range of system information regardless of need. This fact was demonstrated in a recent DoD exercise; an exercise that focused on the DoD's ability to deal with the cyber threat to the Defense Information Infrastructure (DII), and also the DoD's ability to cooperate with the rest of the U .S. Government to deal with threats to the National Information Infrastructure (NII).

When an information operations exercise takes place, two teams of security experts are generally sent out to test the system under investigation. The Red Team is a set of individuals whose task is to act as the adversary and use whatever tools they have available to them to attack the system under test. The Blue Team is a set of individuals whose task it is to use the security tools and procedures already in place to defend the system under test from the attack. The adversarial relationship created in this type of test serves to stress the system under test as it might be in real-world conditions and determine what weaknesses still exist in the system. During a recent exercise, the Red Team force postulated gaining access to a government-wide and government operated classified network. Although the Red Team had no privileges, with respect to access, they were treated by the network as authorized insiders.

The government operated classified network is separated from the rest of the world by a security barrier. This barrier works well; however, if the barrier were to be breached by a hostile user, the privileges enjoyed by the intruder would be the same as those enjoyed by the authorized user. This postulated attack on the network demonstrated that there is little defense once a hostile information operations effort breaks the network security barrier. The network's defense, and its ability to authenticate access, is oriented outward toward the unclassified systems. The networked systems connected to the classified network are generally configured for global permissions. A break through any classified network user connection makes all connected organizations vulnerable because of the network's interconnected nature. This example from a recent exercise highlights the insider threat, since once inside, everyone is considered a trusted agent of the U.S. Government.

The security barriers protecting our classified networks are good and must remain strong, but customer requirements and the insider threat makes an active defensive posture essential for both classified and unclassified systems. Tools, along the lines of intrusion detection, firewalls/secure mail guards, and strong identification and authentication should be enhanced and universally applied. While these tools traditionally have been focused outward, usually protecting against barrier penetration, they should also be applied within the enclave to protect internal nets and even individual

host machines. The insider threat is real and is only complicated by the fact that an outsider can possibly attain insider status by gaining access.

V. COUNTERMEASURES TO THE INSIDER THREAT

11. Countermeasure Objectives

There are many available technical and procedural countermeasures that can help to deal with the insider threat. In order to decide which countermeasures are the most effective and how effective any countermeasure is, it is helpful to first define what the community would like these countermeasures to do. The following is a list of objectives, in decreasing order of effectiveness, that provide some insight into what the community needs to do to deal with the insider threat. These measures are specifically focused on the use (or abuse) of IS by insiders.

a. Define and enforce limits on the overt access to sensitive information and networks. That is, limit the range of authorized privileges (i.e., authorized access to information and information resources) of each individual to a set of privileges consistent with the duties and responsibilities of said individual. The intent is to try to minimize the damage that a malicious insider can cause if the insider decides to compromise information to which he or she has access.

b. Hold individuals accountable for their actions by providing reliable (non-refutable) records of the actions of individuals authorized access to sensitive data and networks. The premise here is that by keeping reliable logs of individual actions, individuals may be deterred from trying to access information unless they have a good rationale for accessing it.

c. Review the actions of individuals. That is, review the audit logs for actions or accesses that seem inappropriate. The reviews should be more extensive and frequent for individuals with higher privileges. It is often counter to our current culture to “check up on subordinates,” because it implies lack of trust and confidence in these valuable employees. However, knowledge that such “audits” occur, even on an irregular basis, acts as a deterrent to unauthorized or inappropriate actions. These audits might be considered the electronic equivalent to the periodic background checks that are performed on individuals as part of personnel security measures.

d. Prevent covert access to sensitive information and networks by making the system security measures resistant to sophisticated attacks by insiders. Malicious insiders may, in certain cases, take the risky steps of trying to bypass an organization's security controls. To counter this, measures are needed to resist more sophisticated network attacks.

e. Detect covert access to sensitive information and networks. Since not all network attacks can be prevented, another objective is to try to detect such attacks by using intrusion detection methods to look for attack signatures or anomalies that indicate a network attack may be in progress or may have already occurred.

f. Quickly and efficiently perform damage assessments, localize damage, and recover in the event that the system security policy has been violated. At best, technical countermeasures can only provide a measure of protection against (and detection of) attacks by insiders. Hence, it is equally important to have plans in place to recover from such penetrations when and if they are detected. These plans need to be supported by technical mechanisms that provide the automated tools to assess damage and select recovery measures.

12. Technical Countermeasures

a. Access Control

Tools and technologies to provide access control services are available from many vendors. The following are some of the most important characteristics that need to be addressed in order to implement effective technical access control measures.

(1) Access control criteria. The individuals and organizations who control access to sensitive data and resources need to have clear policy that guides them in understanding what individuals and organizations should be permitted access to particular types of data and resources.

(2) Access control lists. Using the above criteria, the data owners need to define (based on individuals, rules, roles. etc.) and maintain on a recurring basis, the lists of specific users who are authorized to access each type of data or resource. This typically requires a mechanism for labeling the sensitivity and access control ground rules for various types of data.

(3) Access control enforcement tools. Automated tools must be provided that allow organizations to enter and maintain these access control lists. The tools must also provide effective enforcement of these access control lists. For example, each time a user requests access to a particular file, object, database, etc., the access control tool must determine whether or not the request is authorized and then grant or deny the request accordingly.

b. Identification and Authentication (I&A)

To be effective, access control mechanisms must be able to ascertain the correct identity of each individual requesting access to data or resources. This generally involves two steps. First, obtaining the user's "claimed" identity. Second, forcing the user to authenticate his or her identity. Various I&A options are available from a large number of vendors. They vary significantly in the nature of the mechanisms and in their strength and assurance. The more effective mechanisms require two or three means of

authentication (e.g., password, token, biometric) and are structured to authenticate the entire "session" vice just the initiation of a session. It's important to select an I&A mechanism that has an overall strength that is commensurate with the sensitivity of the data being protected or the action being taken.

c. Encryption

After a user requests data from a server (in a client-server model) and the access control measures have been applied, it is foolish to send the result (the data, file, etc.) unencrypted over the network. If the data is unencrypted, malicious insiders could use sniffers to monitor the traffic on the internal networks and access data intended for another user. Likewise, sensitive data sent from user to user (e.g., messages, files, etc.) needs to be protected from monitoring by insiders without a need-to-know. For these reasons, the ability to encrypt data (user to user, and in client server applications) is an important security service. Application layer encryption is now available from multiple commercial vendors in support of the most popular computing applications. Equally important is encrypting sensitive files stored on hosts and servers. This prevents an insider who manages to access this data from gathering any useful intelligence. Both file and media encryptors (file encryptors encrypt designated flies, media encryptors encrypt all files on a defined media) are available.

d. Operating system controls

The host and server operating systems play a lead role in enforcing the organization's security policy and access control rules. Hence, it is important to use operating systems that provide both flexibility and assurance in the implementation of access control mechanisms. Further, it's important that these operating systems be correctly configured and that they be regularly updated to accommodate security patches and upgrades offered by the operating system providers. The DoD's Common Operating Environment program is an initiative that addresses these issues through tight controls on operating system selection, configuration, and maintenance.

e. System administration tools

One of the most effective countermeasures to the insider threat is to ensure that the individuals who administer the networks (especially the more sensitive networks) are specially selected and highly trained and skilled at ensuring that the organization's security policy is enforced on a 24-hour basis. They also need to be given the time and resources to accomplish this job in addition to their other duties. There are many new tools now available to help these administrators do their job. For example, network vulnerability scanners are available from multiple sources that will assess the configuration of a given network, will identify security deficiencies, and will recommend countermeasures. These tools can also monitor the implementation of password policies.

f. Event Logging and Audit Reduction Tools

To address Objective 3 (Sec. V., para. ll.c.), an organization needs reliable logs of security-relevant events that occur within an organization's information networks. Tools are available to create and maintain such logs both at the operating system level and in support of a number of common networking applications. However, the organization must decide what types of events are worth monitoring and during what times of day. In the event that suspicious activity is detected, the organization also needs to fine tune the event logging tools to record additional events of interest or to adjust the logging thresholds to get a finer picture of suspicious activity.

It is possible for an insider, after having accessed unauthorized data, to cover his or her tracks by modifying the event logs. For this reason, it is important that an integrity mechanism be applied to detect any modification of these logs. This may involve applying a digital signature to individual or combinations of logs with sequence numbers to ensure that the logs are complete.

Of equal, or perhaps greater importance, is the need for tools that analyze event logs and support the auditor in his/her search for suspicious activity. The tedious nature of such reviews, especially when the amount of recorded data can be enormous, often results in a cursory examination at best. However, more sophisticated tools are becoming available to automatically scan large amounts of data and to present suspicious events to the auditor in a more user friendly fashion.

g. Intrusion Detection Tools

Intrusion detection tools typically monitor transactions at the network layer. These tools monitor events based on source and destination addresses and protocol types and can look for "signatures" of known attack scenarios and anomalous behavioral patterns. The more sophisticated tools can respond fast enough to allow system administrators to react in real-time to potential intrusions and to shut down specific ports or entire systems in order to prevent damage from network based attacks.

h. Boundary Protection Mechanisms

The access control measures addressed earlier tended to focus on the hosts and servers within a Local Area Network (LAN). However, many LANs are interconnected not only within an organization's local enclave but across the wide area networks used to create intranets and extranets. While the use of virtual private networking technology can help to protect these environments from outsiders, they do nothing to counter insider threats. In fact, they may make the problem worse. This is because the interconnection provides individuals in remote locations with access to information in one's local system as if the distant user was an authorized local user.

While this may be necessary in certain cases, it is also prudent to limit access to an organization's LAN to those who have a valid need for this access. The installation of boundary protection devices such as firewalls can help to protect local networks both by limiting access as well as by scanning content for potentially harmful mail bombs, viruses, trojan horses, etc..

Mapping of Technical Countermeasures to Objectives

The preceding paragraphs identified objectives and generic countermeasures. The following table provides some additional insight by showing which countermeasures tend to support each objective.

Mechanisms to Support Objectives:

Objective	Technical Countermeasures to the Insider Objectives							
	Access Control	I&A	Encryp-tio	O.S Controls	S.A. Tools	Event Logging	Intrusion Detection	Enclave Boundary Controls
Enforce Access Limits	■	■	■	■	■		■	■
Account-ability		■				■		
Review Actions				■		■	■	
Prevent Covert Access	■	■	■	■	■	■	■	■
Detect Covert Access				■		■	■	■
Recovery	■				■	■	■	

Summary of Technical Countermeasures

Protecting against and detecting malicious behavior by insiders is one of the most difficult information assurance challenges. The good news is that there are in fact many

technical countermeasures available to address this concern. These measures, if properly implemented and administered, can help to limit the damage that an insider can do and can provide a measure of deterrence for at least certain insiders. They can also support damage assessment and reconstitution activities needed to restore operations. Success in using these mechanisms depends heavily on a willingness to limit access on a need-to-know basis. This is somewhat counter to today's culture that tends to support a high degree of open sharing of information. However, organizations that have sensitive information, and that choose to control it carefully, will find that the use of the suggested measures can provide increased protection against the insider threat.

13. Procedural Countermeasures

Ultimately in carrying out governmental missions and in executing the associated responsibilities, we must rely on people to protect networked IS: system administrators, Information Systems Security Managers and Officers (ISSMs/ISSOs), program architects and managers, accreditors, and basic users, among others. It is neither practical nor feasible to rely totally on technology to enforce security; likewise, it is neither practical nor feasible to rely totally on procedures. To be most effective, technology and procedures must complement one another. Although on the surface, procedural countermeasures are cheaper and appear easier to implement, the down side is that they are often difficult to enforce. The government does not have, and will not likely have, a security policy/procedure patrol to ensure that the written rules are not broken. A simple written mandate, for example, requiring users to change passwords every three months often goes unheeded; however, supplementing the written mandate with a technical denial of access to a system if the password isn't changed (after appropriate warning has been provided) is almost always more successful.

A number of commonly-invoked procedures used to protect "valuable" information/IS from outside attacks are described below. These same procedures and more should be considered when dealing with the "insider." Although these procedural countermeasures may be similar to some of the technical ones, the focus is different. ANNEX A identifies some of the policies in place that delineate personnel, security and/or administrative procedures.

a. Personnel Security Procedures

The national interest requires the protection of certain information (classified, sensitive, proprietary, etc.), the disclosure of which could cause irreparable damage to national security, economic damage or loss, and/or possibly the loss of human life. Requirements associated with deciding whether an individual should be allowed access or continued access to classified information often involve the following:

(1) ***Background investigations.*** These are conducted by investigative agencies, i.e., agencies authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information in order to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information. They include:

The disclosure of relevant financial and travel records;
The agreement to adhere to defined rules of personal conduct;
The agreement to sign an approved nondisclosure agreement;
The agreement to submit to an examination via a polygraph; and in many case, U.S. Citizenship.

(2) ***Employee Responsibilities.*** Additionally, once hired and permitted access to classified and sensitive information, employees are required to: protect sensitive and classified information in their custody from unauthorized disclosure; report all contacts with persons who seek to obtain from them unauthorized access to classified information; report all violations of security regulations to the appropriate security officials; challenge when observing suspicious behavior; and comply with other, often more stringent, security requirements designated by their parent organizations.

(3) U.S. Department/Agency Responsibilities. The relationship between the employee allowed access to sensitive information and the U .S. Government department or agency for which that employee works is a symbiotic relationship. The employee must carry out the requirements delineated in the paragraph above; the Department or Agency, in turn, must ensure that there is an established program in place to educate employees about their individual responsibilities; and to assist employees who have questions or concerns about issues such as financial matters, mental health, or substance abuse.

b. Procedures Relating To Users and "Super-Users" (e.g., System Administrators)

In addition to users on a system who should be allowed virtual access to a system based on criteria such as clearance, compartment, and/or need-to-know, a cadre of professionals (e.g., system administrators) have privileges that allow them root access to systems for which they are responsible. These privileges include the ability to: read all files; destroy applications or information; circumvent internal controls; set up and administer user accounts and authenticators; control access of individuals; troubleshoot IS monitoring functions; and (potentially) connect to other systems. System administrators have the ability, because of their position, to virtually control the

operations of an IS. A DoD report from the Office of the Inspector General ("DoD Management of Information Assurance Efforts to Protect Automated Information Systems," dated September 25, 1997) alleges that "system administrators exceeding their roles and responsibilities were among the most common problems associated with insiders exploiting vulnerabilities." That same report showed that 87 percent of identified intruders in DoD systems were employees or others internal to the organization.

Procedures often prescribed to circumscribe virtual accessibility of users (including the super user) into systems include:

A management control program - an outline of the organization's efforts to ensure (1) that management control systems are working effectively through the assignment of responsibilities at the policy level. (2) the issuance and implementation of guidance (e.g., established procedures for tracking those individuals with "super-user" or " root" privileges), (3) the implementation of risk assessments and management control reviews, (4) that there exists provisions for quality control, and (5) that reports are made available to senior management;

Separation of duties - a control process to ensure that a single individual cannot negate the security safeguards of a system;

Least privilege - the principle that requires each user in a system to be granted only the privileges needed for the performance of authorized tasks;

Accountability - the property that enables activities on a system to be traced to individuals who may be held responsible for their actions;

Audits (a means of achieving accountability) - security-related events that allow detection and after-the-fact investigation to trace events and violations to a particular individual; regular reviews and investigation of anomalies discovered in audit data; and retention and adequate protection of audit trails to prevent modification and/ or destruction;

Authentication - positive identification sufficient for permitting certain rights or privileges; identification of users with validated “need-to-know";

Passwords - character strings used to authenticate users' identities; password management; and

Help Desk Capabilities - to assist users with questions or experiencing problems; and education, training, and awareness programs, including initial orientation, more advanced education and training commensurate with duties and responsibilities, and reinforcement activities. (NOTE: For many personnel with critical system responsibilities, e.g., system administrators, such responsibilities are often “other duties as assigned.")

c. Policies Relating to the Protection of Information Systems

country's vulnerability. IS, for the most part automated and interconnected, are dependent on critical infrastructures (e.g., telecommunications, energy, emergency services) which historically have been physically and logically separate. To address the protection required, PDD-63 includes as its goal eliminating any significant vulnerabilities to critical infrastructures, especially cyber-based IS, by the year 2003. Subject to nontraditional attacks that could cause significant harm to our military power and economy as well as disruption of vital services, critical infrastructures often fall under the purview of both the government and private sectors; thus, PDD-63 mandates that the government work in partnership with the private sector in planning for and protecting identity infrastructures. To reduce the potential increase in vulnerabilities within the Federal Government. PDD-63 mandates every U.S. department and agency accomplish the following:

- Designate its Chief Information Officer as the individual responsible for information assurance;

- Appoint a Chief Infrastructure Assurance Officer to be responsible for all of the other aspects of that department's/agency's critical infrastructures;

- Establish procedures to obtain validated vulnerability assessments on government computer and physical systems;

- Develop a plan for protecting its critical infrastructures. Submitted to the National Coordinator for analysis of inter-governmental dependencies and mitigation of those dependencies, the plan is to be updated every two years.

Disruption in the flow of vital U.S. Government information, a critical vulnerability, is addressed by a recently-released Executive Order (E.O.) 13073 (February 1998) concerning Year 2000 conversions. In addition to establishing a Year 2000 Conversion Council, E.O. 13073 mandates that no critical Federal program experience disruption because of the Y2K problem. Another E.O. 12864 (September 1993) establishes within the Department of Commerce the United States Advisory Council on the National Information Infrastructure, the purpose of this council being to advise the Secretary of Commerce on matters related to the development of the NII, including national security and emergency preparations.

OMB Circular A-130, Appendix III, "Security of Federal Automated Resources" delineates requirements to all U.S. Government departments and agencies in the protection of Federal Government IS. Prescribed safeguards addressed in this Circular include:

- Ensuring information is protected commensurately with the potential risk and magnitude of harm;

- Limiting the collection of information to authorized individuals and allowing such collection only when necessary for the proper performance of agency functions;

- Limiting the sharing of information to authorized individuals;

- Training personnel in skills appropriate to their roles in the management of information;

- Providing for periodic review of information systems to determine: how the mission may have changed; whether the IS continues to fulfill ongoing and anticipated mission requirements; and the level of maintenance needed to ensure the IS meets the mission requirements cost effectively; and

- Ensuring that the official who administers a program supported by an IS is responsible and accountable for the management of that IS throughout its life cycle.

Although the OMB Circular provides a generic overview of requirements relating to protecting the U.S. Government's IS, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) has promulgated numerous issuances (e.g., policies, instructions, advisory memoranda) that address in more focused detail particular security-related requirements. NSTISSC issuances, national in scope, have covered a broad range of issues, a subset of which include:

- Use of Cryptomaterial by Activities Operating in High Risk Environments;

- Education, Training, Awareness --a series of documents for personnel with significant roles (e.g., Accreditors, System Administrators, Information Systems Security Officers);

- Certification and Accreditation of National Security Telecommunications and Information Systems;

- Electronic Keying;

- Government Contractor Telecommunications;

- Incident Response and Vulnerability Reporting for National Security Systems;

- Compromising Emanations;

- Communications Security Monitoring; and

- Doctrines for operating various INFOSEC equipment.

In its goal to maintain relevancy in concert with the rapid evolution of technology, the NSTISSC hosts an annual offsite that addresses key issues and initiatives and also sponsors national-level issue groups (e.g., Information Assurance; Education, Training, Awareness) to focus on areas of particular concern.

With the existing and newly-implemented policy protection initiatives, it should be pointed out that ***none*** explicitly relate to addressing the "insider threat" problem. Departments and agencies implement the policies and procedures mandated in national and departmental issuances and develop, as appropriate, their individual, application-specific security policies.

d. System Security Policies

A security policy is the set of laws, rules, and practices that regulate how an organization protects its IS and the data within them. Its development is

based on national and departmental requirements factored into specific applications and environments. Often the baseline requirements center around the triad of critical information characteristics of confidentiality, integrity, and availability:

Confidentiality -the assurance that only selected users or groups (based on their responsibilities, privileges, and need-to-know) are allowed access to certain data;

Integrity -the assurance that data in the system is accurate and complete, and hasn't undergone unauthorized (accidental or malicious) modification or destruction; and

Availability -the assurance that the system works reliably, and the data in the system is accessible to authorized users when requested or needed. If adhered to, the composite of procedural countermeasures mandated in the national and defense policy issuances, when incorporated into security policies, would help control or minimize the insider threat problem. Procedural requirements cited in such policies are often a subset of the following:

(1) Access controls

- Virtual access controls and tools, including the establishment of an access authorization process and account and password management; limitations on group accounts (lists of individuals that are part of group); the delineation of tools available to the general user population (e.g., virus detection software) and those tools limited to certain authorized users (e.g., network analyzers); isolation of operating system via partitions, domains, etc. to prevent introduction of malicious codes;

- Physical access controls and tools, including the location of critically-sensitive components and material in controlled locations or facilities with physical security parameters in place to protect critical network nodes (e.g., communication circuits, termination points, entry points); alarms; intrusion detection

within applications, operating systems, and at network layer; procedures required for attended and unattended operations of IS; regular checks of the hardware;

(2) Accountability for classified and/or sensitive material and data (including marking and handling of the data) and documentation controls; secured distribution of sensitive account information (e.g., passwords);

(3) Configuration management limiting the number of authorized personnel (or approved, designated contractors) allowed to make system changes and documenting those changes;

(4) System connections and controlled interfaces (e.g., firewalls, guards) between interconnected systems;

(5) Maintenance procedures for local employees and contract employees (cleared and/or escorted and supervised by knowledgeable personnel), including the review of maintenance diagnostics before they are executed on the system;

(6) Reportable incidents, violations, compromises; suspected unapproved activities; suspected network attacks; and consequences for failing to comply with departmental rules;

(7) Procedures associated with magnetic media (e.g., shareware, personal software, virus checks, overwrites, purging, degaussing, storing, transporting, destruction); periodic inventories to account for sensitive material;

(8) Contingency procedures / continuity of operations / disaster recovery (these plans and procedures may entail storage of critical backup media offsite); and

(9) Legal issues relating to monitoring, work-related management searches; file transfers; workplace practices (e.g., the log-on banner); personal use of government software in support of nonwork activities, downloading, and the like.

Summary of Procedural Countermeasures

Numerous policies in place, at the national, defense, service, and agency levels, prescribe procedural countermeasures to protect valuable information in U.S. Government systems. Although most of these procedures have been mandated for years, many of them are not enforced and/or are not properly implemented. Moreover, the focus of the policies and mandated procedures has been directed toward preventing entry by outsiders into U.S. Government systems.

Equal, if not more, focus will need to be directed toward ensuring that insiders are prevented from doing harm to the Government's systems. DoD's IG Report, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," dated September 25, 1997 recommended including accountability for management control practices in the job descriptions, performance plans, and performance evaluations of personnel responsible for safeguarding DoD's IS. This recommendation is in concert with both the Government Performance and Results Act, that is intended to increase federal program effectiveness through strategic planning and performance-based management; and the Defense-wide Information Assurance Program (DIAP), one of the desired outcomes of this program being the establishment of performance measures based on effective, measurable criteria.

VI. RECOMMENDATIONS

Having taken a look at threats and vulnerabilities posed by the insider against Government IS, and the various countermeasures - both technical and procedural - that might be used to mitigate the risks associated with those insiders, the following

recommendations are offered as immediate steps to improving this situation. As noted earlier, these recommendations are offered in priority order with some emphasis placed on ease of implementation and cost. The order is, however, subject to several considerations that might influence the final outcome. One discriminator would be the issue of deterring an existing insider versus that of deterring someone who might become an insider. Another would be the need to show a serious resolve in the short term, versus taking a longer term, strategic approach to this problem. The important point is that all are positive steps that would improve our posture with respect to the insider threat, and that minor adjustments in order are less significant.

14. Enforce Policies Already in Place

Many policies relating to personnel security, computer security, and IS security mandate security procedures to protect mission-critical information (e.g., classified, sensitive), the unauthorized disclosure of which could irreparably harm the United States' security and economy and could potentially result in the loss of privacy or in the premature loss of life. The management control program established by each government organization is required to ensure that there are effective procedures in place: the assignment of responsibilities; the issuance and implementation of guidance; the conduct of risk assessments and management control reviews; the provision for quality control; and reporting to senior management. An essential element of an effective security program is accountability. Those individuals responsible for an action must be held accountable when IS are not in compliance with prescribed security requirements and when known security vulnerabilities have not been corrected.

15. Enforce National and Organizational Policies that Mandate the Establishment of a Security Policy for All Systems

U.S. Government information technology has evolved from stand-alone mainframe computers to an intricate, seamless web of communication networks, computers, software, databases, security services, and other processes. Risk to one organization now represents risk to all and, from a lessons-learned perspective, we are cognizant of the internal and external threats to our systems. As more and more systems throughout the government are interconnected, it is incumbent on all U.S. Government departments and agencies to adhere to OMB Circular A-130. Appendix III that requires security plans for all government systems. U.S. Government departments and agencies cannot assume that the insider threat problem is too difficult to solve and, thus, should not be tackled. System planners must consider controls (e.g., evaluation tools, contingency plans, manageable audits) to mitigate the growing number of insider problems.

16. Security Education, Training, and Awareness (ETA) Programs Should Be Mandatory for All Users and Employee Assistance Programs Must Be Enhanced

ETA programs must provide a rationale for the rules and regulations that are being enforced. This training must not only identify the punishment to the individual,

but must also clearly identify the impact to others, the organization, and the nation that can result from failure to follow these rules and regulations. It is recommended that training take the OPSEC approach and provide instruction in identifying critical information and the need to protect it. When personnel understand the need for rules and regulations, they comply more readily. This training should be reinforced through warning banners, posters, daily reminders, publications, and through discussions in other training classes. Information developed from the psychological profile might be provided during training sessions. It also recommended that the outcome of infractions that have been adjudicated be publicized throughout the organization (names and case files should not be identified) to reinforce the fact that not only is there a problem, but that it is being addressed. Employees who are identified as potential computer abusers must be provided with enhanced assistance in the areas of psychological problems, monetary problems, marital and family problems, etc.

17. Access Controls

Systems that process classified and sensitive information need to enforce mandatory and discretionary access control mechanisms to ensure that only users with the proper clearances and need-to-know are able to access this data. The need for access as well as access permissions should be reviewed periodically. Access control mechanisms need to be deployed not only at network boundaries (to control external access), but within the client-server computing environment (to limit insider access). The use of such mechanisms requires that appropriate data labels (or other mechanisms) be used to identify the access control ground rules - for individual files, messages, databases, etc. Until viable mandatory access control mechanisms become widely available, systems processing different levels of information must remain isolated and each enforce discretionary access control.

18. Strong Authentication

Access control mechanisms are critically dependent on the authentication mechanism used to validate the identity of the users requesting access. It is well known that reusable passwords (today's most prolific authentication mechanism) are highly vulnerable due to their unprotected nature and due to poor operational practices. A major initiative is needed to replace passwords with strong authentication mechanisms that require the use of tokens or biometrics (for user login) and cryptographic authentication (for network interactions). As an interim measure, the administration of password-based systems needs to be significantly strengthened both procedurally and with automated tools (such as network vulnerability scanners).

19. Establish Senior Focal Point for Security in AIS

Assign a senior individual in each government department or agency with responsibility to oversee department/agency monitoring of employee computer use (e.g.,

a Chief Information Officer (CIO) Security). This senior could also serve as the champion and mentor for system administrator professionalization and development and for workforce training in IS security.

20. Establish Personnel Security Vetting Procedures Commensurate with Individuals' Level of IS Access

Individuals with privileged, root, or super-user access should be given additional attention. It is particularly important to focus on developing a strong security partnership with system administrators, ensuring that these individuals receive the best security awareness training available. Career development programs and industry accepted certification or licensing should be initiated. For government elements that have authority to polygraph personnel, more frequent polygraphs are recommended for individuals with greater IS access. Polygraphs could be supplemented by the creation of a special access program, including a security file review, for individuals with privileged access. For government elements without polygraph authority, additional emphasis should be given to background investigations.

21. Select, Train, Motivate and Reward System Administrators

System administration is a critical function and point of vulnerability. As such, the government must be more selective in who it assigns to system administrator positions, how it screens and monitors people in these positions, and how it regards system administrators. Prospective or current system administrators should receive additional screening during background investigations and more frequent polygraphs. Use of a "Psychological Profile" tool may be helpful in recruiting "trusted" individuals for system administrator positions. Once hired, they need a defined career path. They should be provided on-the-job training and individually tailored training plans to include ethics training. In an effort to keep skills current, they should be afforded every opportunity to attend technical and security related courses. They should not be assigned other job functions that may interfere with their system administrator duties. Finally, in order to motivate and retain valued system administrators, a special pay scale or rewards program (e.g., SA of the Quarter or SA of the Year) should be instituted.

22. File Encryption

Unprotected data stored on user workstations and data servers is vulnerable to a number of insider attacks. To counter this, organizations should be encouraged to widely deploy media or file encryptors that transparently encrypt sensitive data. Particular attention needs to be paid to the mechanisms that generate and store the key encryption keys used for this purpose to ensure that they are resistant to insider attacks. In addition, data recovery mechanisms need to be used to ensure that the encrypted data can be recovered (by appropriate authorities) in the event of a lost or damaged token or other failure condition.

23. Collect and Analyze Audit Data on Use of IS and Perform Audits

Scrutinize the online activities of individuals with root privilege and/or broad “need-to-know" access. This will be costly and labor intensive, but the real threat of audits can do much to deter the insider problem. Auditing can establish normal computer use profiles, and thereby enable the detection of abnormal patterns. The development of additional audit/profiling tools, such as an icon that would alert the user to ongoing monitoring could assist this effort. Additionally, auditing the use of printers and other removable media would disclose the removal of large quantities of data.

24. Deploy Intrusion Detection Tools for Use Within IS

Intrusion detection should also focus on the malicious and mischievous activity of the insider. It should be positioned at multiple levels within a system (e.g. local workstation, host levels). Traditionally, our intrusion detection systems have focused outward, protecting against an attack from the outside while ignoring the security aspects of monitoring for active attacks on the inside. Special attention should be given to detecting anomalous insider activity, activity associated with not only entry into and within a system, but also egress from the system.

25. Establish a Repository for the Sharing of Insider Attack Information

This should, as a minimum, include relating hacker activities, viruses, incidents, incident responses, reports concerning incidents, and lessons learned. Vulnerability and incident databases are being developed by the computer emergency response team community for hacker-related activity, but this is not focused on the insider problem. A similar capability to amass and share incident information related to the insider would raise the awareness level of the community to the threat posed by the insider and also educate the community as to the symptoms that would alert one to an insider attack.

26. Develop a Psychological Profile of an Insider to Assist in the Early Identification of Future Insider / Computer Abusers

This profile should provide managers, security specialists, and medical personnel a profile of the insider/computer abuser thus enabling them to identify potential abusers before they cause serious damage. Employees should be instructed in reporting employee changes, both on the job and off the job, to their management chain. The profile should be developed based on known insider/abusers and should be automated, to the degree possible, to assist in the detection of profiled activities. Studies are underway to develop such a profile, and they should be continued. Once developed, this profile will assist in the development of questions for security investigations and will also provide additional material for security education, awareness, and training.

27. Stop the Practice of Publishing Sensitive Data on Unclassified Databases, Web Sites, etc.

Data that is being released into unclassified databases or web sites must be reviewed for sensitivity prior to release. Existing programs specify the method for releasing data to the public. Placing information in unclassified databases and on web pages is literally the same as publicly releasing the data. This data must be reviewed in the aggregate; that is, a determination must be made as to whether this "unclassified" data when combined with the other "unclassified" data being released or already publicly available will reveal critical information or provide a road map to attacking the system. Internal unclassified databases must be provided strong access controls to restrict "pull technology" by those without a justified need-to-know. In addition, the intranet and other internal Agency and Community networks offer opportunities for knowledgeable personnel to glean and aggregate information of value within closed communities. What is now required of corporate information officers within their spheres of responsibility is the requirement to review the balance between making information fully and readily available (unless precluded by defined restrictions) and security. Some semblance of editorial control over content and determination of “need-to-know" should be taken into consideration.

28. Increase Security Associated with Physical Access

Physical security and physical access controls must be enhanced. State-of-the-art technology, such as biometrics, must be implemented - we must move beyond the days of "flashing a badge" or personal recognition. Personnel with a clearance, but not the need-to-know, must be escorted and their activities controlled within sensitive areas. Security must be evenly applied to all ranks and grades with no one being exempted by virtue of higher rank or position. Enhanced sensory devices should be developed to detect physical intrusion. Sensitive areas must be swept-even in the continental U.S. Sweeping should not be conducted on a predictable schedule. It should be done randomly.

29. Conduct Independent Vulnerability Assessments

Independent vulnerability assessments--from the broad system level assessments to penetration testing to red teaming--are a good way to periodically check the security health of IS. These assessments need to encompass all aspects of insider threats and vulnerabilities. Checking the organization's progress in implementing the recommendations in this advisory is a good way of doing this.

Encl:
ANNEX A

ANNEX A -Procedural Countermeasures: Insider Threat

With all of the advances in technology, we ultimately depend on PEOPLE with varying roles and responsibilities to protect government networked information systems. Examples of important roles involved in our systems include administrators, Information Systems Security Managers and Officers (ISSMs/ISSOs), Program Architects and Managers, and Users.

On global, national, intelligence, and defense scales, we recognize that the unauthorized disclosure of certain information (e.g., classified, sensitive, proprietary, etc.) can cause irreparable damage to the nation's security and economy, as well as result in the loss of human life.

Existing policies that address some aspect of this problem include:

•**E.O. 12958**, "Classified National Security Information" (delineates what is considered classified, safeguarding procedures, etc.)

•**P.L. 100-235**, "Computer Security Act of 1987" (delineates what is sensitive, the need to protect sensitive, roles/responsibilities)

*Agencies are to invest in information systems only after determining that the risk and expense of the systems meet agency needs not just to “keep up" with other agencies

*Mandates security training for those responsible for government information systems.

•**E.O. 12968**, "Access to Classified Information" (delineates personnel security requirements)

* Employees shall not be granted access to classified information unless they: have been determined to be eligible for access...based upon a favorable adjudication of an appropriate investigation of the employee's background; have a demonstrated need-to-know; and have signed an approved nondisclosure agreement.

•**OMB Circular A-130, Appendix III**, "Security of Federal Automated Resources" (delineates requirement to protect all U.S. Government information systems, defines roles/responsibilities, plan for security, etc.). Safeguards addressed include:

* Ensuring information is commensurate with the risk and magnitude of the harm ...;

* Limiting the collection of information that identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

* Limiting the sharing of information to authorized individuals;

* Ensuring users having the skills, knowledge, and training to manage information resources…;

* Training personnel in skills appropriate to management of information; model for two levels of knowledge: awareness level and performance level.

*** NSTISSI No.4012**, "National Training Standard for Designated Approving Authority (DAA)," dated August 1997, establishes the minimum training standard for the development and implementation of training for a DAA of telecommunications and information systems. This instruction identifies a minimal performance standard for the DAA in executing the responsibilities of the accreditor.

*** NSTISSI No.4013**, "National Training Standard for System Administrators in Information Systems Security (INFOSEC)," dated August 1997, establishes the minimum training standard for the development and implementation of training for System Administrators in the disciplines of telecommunications and information systems security .

Principles espoused in PDD-29, "Security Policy Coordination," dated September 16, 1994:

- Our security policies and services must realistically match the threats we face and must be sufficiently flexible to facilitate change as the threats evolve.

- Our security policies and practices must be consistent and enable us to allocate scarce resources effectively.

- Our security standards and procedures must result in the fair and equitable treatment of all Americans upon whom we rely to guard our nation's security.

- Our security policies, practices and procedures must provide the security we need at a price we can afford.