Audit Report

OFFICE OF THE INSPECTOR GENERAL

SECURITY CONTROLS OVER SYSTEMS SERVING THE DOD PERSONNEL SECURITY PROGRAM

Report No. 98-024 November 19, 1997

Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DAA	Designated Approval Authority
DCII	Defense Clearance Investigative Index
DIS	Defense Investigative Service
LAN	Local Area Network
MOA	Memorandum Of Agreement
NSA	National Security Agency

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

November 19, 1997

MEMORANDUM FOR DIRECTOR, DEFENSE INVESTIGATIVE SERVICE

SUBJECT: Audit Report on Security Controls Over Systems Serving the DoD Personnel Security Program (Report No. 98-024)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments on a draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. As a result of management comments, we deleted draft Recommendation 3. No additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Tom Gimble, Director, Acquisition Management Directorate, at (703) 604-9000 (DSN 664-9000) or Mr. J. David Stockard, Audit Team Leader, at (703) 604-9016 (DSN 664-9016). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-024 **November 19, 1997**
(Project No. 6RD-5049.02)

Security Controls Over Systems Serving the DoD Personnel Security Program

Executive Summary

Introduction. The DoD established the Defense Investigative Service (DIS) to administer the investigative portion of its personnel security program. The DIS uses a network of computer systems to collect, track, adjudicate, and disseminate information about individual security clearances for over 15 million individuals. The network is primarily located at the DIS Personnel Investigations Center in Baltimore, Maryland, and is administered by the Information Services Division of the DIS.

Audit Objectives. The overall audit objective was to determine the effectiveness and efficiency of the management of the DoD personnel security program. The objective of the segment of the audit addressed in this report was to evaluate security controls over computer systems serving the DoD personnel security program.

Audit Results. The DIS has taken actions to implement encryption technologies and an internet firewall (a system or combination of systems that enforce a boundary between two or more networks) to protect its network from outside attacks. Nevertheless, the DIS did not have adequate controls in place yet to protect personnel security systems and data from compromise. As a result, there was still insufficient assurance that unauthorized individuals could be prevented from accessing, modifying, or destroying the highly sensitive DoD personnel security information that DIS administers. Implementation of recommendations will improve security and protect those critical information systems. The management control program could be improved. We identified a material weakness applicable to the primary audit objective (Appendix A).

Because of their sensitive nature, the access control deficiencies discussed in Part I of our report are discussed in general terms only. Details of our findings were separately provided to DIS management.

Summary of Recommendations. We recommend that the Director, Defense Investigative Service, communicate specific security requirements, modify memorandums of agreement and contracts to include system security, develop and implement access control policies, isolate critical resources in the system architecture, and improve physical security.

Corrective Actions Taken. DIS made significant improvements in system security and architecture during the audit. We believe that the security improvements that DIS is currently in the process of implementing will significantly improve system security and reduce the likelihood of a successful system attack. DIS also initiated action to correct the management control weaknesses that led to its security problems.

Management Comments. DIS management concurred with all but one of the 10 recommendations and have initiated actions to correct identified weaknesses. DIS did not concur with the draft recommendation to reposition their Information Systems Security Officer to obtain greater autonomy and objectivity. We have eliminated this recommendation from the final report because of the actions taken or planned in response to the other recommendations. DIS also disagreed that their network was vulnerable to attack, stating that the National Security Agency (NSA) had conducted a penetration review in April 1997 and found only minor problems. See Part I for a complete discussion of management comments and Part III for the complete text of the management comments.

Audit Response. Management's comments to the recommendations were responsive; however, we cannot agree that DIS systems were adequately protected when the audit was conducted, or have yet reached the assurance levels needed for such systems. Both our review of the DIS network and the National Security Agency's review revealed multiple avenues for outside attacks that could be launched against the DIS network. Further, our analysis of the DIS DCII server, the most critical portion of the DIS network, revealed as many as twenty-four different system-level weaknesses that could have allowed a relatively unsophisticated outsider to circumvent security. We reviewed the National Security Agency report in August and noted that its findings substantially agreed with ours.

DIS told us that server weaknesses were corrected September 16, 1997. Correction of critical architecture weaknesses, however, is not scheduled until February 1998. Based on our findings, and on those of the National Security Agency, we believe that the DIS network continues to be vulnerable until those critical architecture weaknesses are corrected.

Table of Contents

Part I - Audit Results

Audit Background

This report is the second in a series on the DoD personnel security program. The first report addressed the overall management of personnel security investigative process by the Defense Investigative Service (DIS) and discussed the various improvements being made during ongoing business process reengineering efforts.

Personnel Security Program. The DoD established its personnel security program to ensure that granting Federal employees, military personnel, contractor employees, and other affiliated persons access to classified information is clearly consistent with the interests of national security. The DoD established the DIS to administer the investigative portion of that program.

Computer Systems Used by DIS. The DIS uses a network of computer systems to collect, track, adjudicate, and disseminate information about individual security clearances within the DoD for over 15 million individuals. The network is primarily located at the DIS Personnel Investigations Center in Baltimore, Maryland, and is administered by the Information Services Division of the DIS. The network consists of multiple local area networks, several midtier[1] computers, and a mainframe computer system (soon to be phased out) which contains the Defense Clearance Investigations Index (DCII) legacy[2] application. The DIS network has multiple points of access, including an internet gateway, dial-up lines (protected by encryption technology), and direct connections to other user organizations. DIS plans to use encryption technologies and an internet firewall (a system or combination of systems that enforce a boundary between two or more networks) to protect that network from outside attacks.

---

[1]A midtier computer is one that is smaller than a mainframe yet still serves multiple users. Midtier computers are often used to administer simple databases because they are generally more cost-effective to operate than a mainframe.

[2]A legacy application is a computer program that is nearing the end of its useful life and is being phased out.

The DCII Database. The DCII is the application that DIS plans to use to store and process all DoD personnel security clearance information. The DCII stores and processes personnel files for security clearances and adjudications. The files include personal information such as credit reports, criminal histories (including expunged records), and medical and mental health records for all DoD military and civilian employees with current or prior DoD security clearances. The Privacy Act of 1974 and the Computer Security Act of 1987 provide requirements and criteria for protecting personal information from public disclosure.

Audit Objectives

The objective of this audit was to evaluate security controls over computer systems serving the DoD personnel security program. Specifically, we:

- evaluated the process for maintaining security over computer systems used by the DIS to conduct personnel security investigations, adjudicate security clearances, and disseminate information related to personnel security investigations;

- analyzed controls preventing unauthorized disclosure of highly sensitive DoD personnel information and critical national security data; and

- analyzed the effectiveness of security and administration of computer processing facilities serving those systems.

See Appendix A for a discussion of the audit scope and methodology. Prior audits and other reviews are discussed in Appendix B.

Strengthening Controls Over DoD Personnel Security Systems

The Defense Investigative Service was working to improve its information assurance posture, but did not yet have adequate controls to protect personnel security systems and data in accordance with applicable standards.

The controls were not adequate because DIS did not effectively communicate security policies and implement security procedures to adequately protect the agency's critical automated information systems. Those management weaknesses led to serious deficiencies in access controls[3]. DIS also needed to improve its network architecture and physical security to more effectively protect its critical systems and data.

As a result there was insufficient assurance that unauthorized individuals could be prevented from accessing, modifying, or destroying the highly sensitive DoD personnel security information that DIS administers.

Standards for Control Over Sensitive Systems

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, (DoD 5200.28) provides policy for safeguarding classified, sensitive unclassified, and unclassified information processed in automated information systems. DoD 5200.28 provides mandatory, minimum automated information system security requirements. DoD 5200.28 states that an automated information system must have a C2 level of protection if the system processes sensitive unclassified information requiring controlled access protection, such as the personnel information and privacy

[3]Access controls are the logical features of a computer system, including software and hardware, that prevent unauthorized access, modification, or destruction of the data that is stored and processed by that computer system.

act data processed by DIS. DoD 5200.28 also requires the appointment of a Designated Approval Authority (DAA) who has ultimate responsibility for the security of the system.

C2 Level of Protection. DoD Standard 5200.28, "DoD Trusted Computer System Evaluation Criteria," December 26, 1985, (DoD 5200.28-STD) defines system security classifications for all DoD systems, and specifies system requirements for each classification. The C2 level of protection mandated by DoD Directive 5200.28 for most DoD unclassified systems is described in detail in DoD 5200.28-STD. The standard defines a system with a C2 classification as one that makes users individually accountable for their actions through procedures for login, auditing of security related events, and isolation of resources. Among other things, the standard requires a C2 system to protect information from access by individuals unless a need to know exists on the part of that specific individual. Other C2 requirements of DoD 5200.28-STD include:

- controlling propagation of access rights,
- protecting authentication data so that it cannot be accessed by unauthorized users,
- implementing a computer operating system that protects itself from external interference or tampering,
- isolating resources to be protected, and
- implementing hardware and software features ensuring system integrity.

Designated Approval Authority. DoD 5200.28 requires the appointment of a Designated Approval Authority (DAA) who has ultimate responsibility for the security of the system. The DAA is appointed by the agency or component chief, and has ultimate responsibility for the security of the agency's automated information systems. The DAA reviews and approves security safeguards, certifies and accredits agency systems, and appoints the Information Systems Security Officer. The DAA for DIS systems is currently the agency Deputy Director.

Communicating Security Policies to Systems Staff, Users, and Contractors

While DIS had well defined security objectives for its computer networks, those objectives had not been effectively communicated to systems staff, user organizations, and contractors through implementation of a detailed Trusted Facility Manual. DIS had also not formalized those objectives in Memorandums of Agreement (MOAs) with its user organizations to ensure that those organizations understood their responsibilities in accessing DIS systems.

DIS Security Objectives. DIS systems security objectives are driven by DoD Directive 5200.28 and by critical personnel and privacy act data on its network. That directive mandates a C2 level of protection. DIS also informally acknowledged that the sheer volume of sensitive information suggests that its DCII system data should potentially be protected at a higher level than C2. At the very least, the volume of sensitive data merits strict implementation of the C2 standard. In preliminary briefings with us, DIS managers believed their systems should be protected at the C2 level. The managers also told us that DIS systems were protected at, or close to, the C2 standard.

Trusted Facility Manual. DIS can effectively communicate its security objectives to systems staff by implementing a detailed Trusted Facility Manual. A Trusted Facility Manual is a management document that communicates the specific intended level of security for a trusted system, specific resources to be protected, and specific technical functions that should be controlled. A Trusted Facility Manual is required by DoD 5200.28-STD, which states:

> Trusted Facility Manual . . . A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

Without the guidance of the manual to specify the level of security, DIS systems administrators implemented security controls that did not adequately protect critical portions of the DIS network. The affected portions of the network included the DEC 8400 Unix Server. This server contains the DCII database that DIS uses to process sensitive personnel information. The deficiencies would have allowed any user or a

knowledgeable outsider to gain access into the highly sensitive DoD personnel security information that DIS administers, and to access, modify, or destroy data without leaving an audit trail.

There is a standard Trusted Facility Manual in use by the DoD that DIS could adapt for its own use with minimum effort. The Defense Information Systems Agency, Western Hemisphere, "Unix Security Technical Implementation Guide, Version 1, Release 2," August 1, 1996, provides technical implementation guidelines to assist the Defense megacenters in meeting the minimum requirements, standards, controls, and options that must be in place for the unix operating system. While this standard does not directly apply to DIS, DIS has the same protection requirements for its systems as the Defense Information Systems Agency. Use of this guidance by DIS, with appropriate changes, would save management the time and effort of drafting similar guidance for its organization.

DIS User Organization MOAs. DIS provides DCII access to organizations within DoD components, including the Army, Navy, Air Force, and several Defense agencies. DIS also planned to provide DCII access to the Office of Personnel Management. Those accesses are administered under MOAs with the organizations. The MOAs written by DIS did not contain provisions stipulating the level of security that the organizations should maintain over their DCII connections. The MOAs contained no DIS security monitoring provisions, and no provisions to disconnect the service if the organization failed to maintain adequate security controls. As a result, the organizations had no requirement to maintain adequate security. Further, DIS had no recourse if it determined that sufficient security was not being maintained. DIS management agreed that such provisions should be included in future MOAs, and stated that this would be the policy. In the case of the pending connection with the Office of Personnel Management, DIS agreed to modify the MOA to include those security provisions. Further, based on our recommendations, DIS contracted with the National Security Agency to perform a security review of the Office of Personnel Management mainframe system before the connection would be allowed.

Need to Implement Security Procedures

The DIS did not implement formal security procedures to protect its critical information systems. Instead DIS had a draft security manual that assigned responsibilities for system security in general terms, without specifying procedures for protecting the systems. DoD 5200.28 states:

> It is DoD policy that, . . . the safeguarding of information and AIS resources . . . shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental [safeguards] . . . . There shall be in place an access control policy for each AIS [Automated Information System]. It shall include features and/or procedures to enforce the access control policy of the information within the AIS.

To effectively protect its systems, DIS needs to develop and implement an access control policy with specific procedures for:

- ensuring that system security is implemented to the appropriate level,
- establishing a baseline of critical system settings to guard against unauthorized changes, and
- monitoring its systems to detect and react to attacks and compromises.

Access Control Policy. A formal access control policy, including documented security procedures, is critical to the successful management of system security. Security procedures allow administration of security to be a management process rather than a technical one. Without procedures establishing a measurable security level and stipulating periodic recertification, management's only recourse is to delegate responsibility for security matters to technical personnel. An appropriately written access control policy actively involves organization management in the daily administration of its systems' security. Periodic review and certification against an established standard allows the manager to determine the effectiveness of protective measures and independently assess whether the measures are adequate. Without a review and certification policy, management can only rely on the judgment of technical personnel regarding adequacy of protective measures.

Security Implementation Procedures. To effectively protect its systems, DIS needs to develop and implement specific procedures to ensure that system security is implemented to the appropriate level. When DIS implemented its new systems, management delegated system security to technical personnel. Procedures did not ensure that technical personnel implemented system security to the appropriate level. Instead, each level of the organization made a judgmental assessment of the "adequacy" of system security. As a result, DIS management believed that system security was implemented to a certain level, when in fact technical staff had implemented at a much lower level.

DIS management believed that its systems were secure. Management felt it had effectively communicated security goals to technical personnel, delegated authority appropriately, and achieved security objectives. However, because management did not have formal procedures to keep it actively involved in security administration, it lost control of that function. Faced with competing priorities, it appears that technical staff chose to accept risks that management would not have accepted. As a result, although DIS managers believed the systems to be well protected, critical portions of the DIS network contained serious security deficiencies and management was not aware of the problem. The affected portions of the network included the DEC 8400 server, which contains the DCII database that DIS uses to process sensitive personnel information. The deficiencies would have allowed any user or a knowledgeable outsider to gain access into the highly sensitive DoD personnel security information that DIS administers, and to access, modify, or destroy that data without leaving an audit trail.

DIS managers would be able to delegate the performance of security related tasks, without giving up either control or visibility of security related issues, if they implemented security procedures establishing a measurable security level and stipulating periodic recertification.

Security Baseline Procedures. DIS procedures did not require management to implement and maintain a system security baseline (baseline). As a result, the agency did not have a basis for effectively monitoring its system against attack, and could not determine if an attack had occurred.

A baseline is a listing of all critical system security settings and security related files. It is recorded at system generation and at the conclusion of a successful recertification effort, and stored in a secure location. A baseline serves in a dual capacity to maintain system security. First, a baseline is periodically compared to the in-place system to determine if unauthorized changes have been made to system security settings. The

presence of unauthorized changes is often the only indicator to a security administrator that a system's security has been compromised. Second, a baseline is used to restore system security after unauthorized changes have been detected. A baseline allows quick restoration of the numerous security settings and files that ensure system security.

The DIS DEC 8400 server had system settings that were questionable and in some cases that compromised system security. Those settings could have resulted from inexperienced system administration, operator error, or intentional unauthorized changes. It was impossible to determine the origin of the questionable settings because DIS did not have a system security baseline. Further, the lack of a baseline made it unnecessarily difficult to restore the system to a secure state.

System Monitoring Procedures. DIS needs to develop and implement specific procedures for system monitoring to detect and react to attacks and compromises to effectively protect its systems. Periodic monitoring activities, whether manual or automated, help protect a computer network against attacks and compromise attempts. DIS did not have a formal policy to conduct those activities with specific responsibilities, reporting requirements, and timelines although DIS performed some monitoring activities on an informal basis.

System monitoring is a two stage process. First, the computer system and network must be configured to log all commands and system actions that could be used to attack or compromise system security. Second, those records must be reviewed on a periodic basis and compared against a system baseline (discussed above) to determine whether an attack is in progress. Those reviews can either be manual or automated. A manual review involves a system security administrator opening each log file and scanning it for suspicious activities. Alternately, a program that performs automated reviews of log files can be programmed in house, or purchased from a vendor. Frequent and regular review of system logs is critical to maintaining system security. Reviews must be frequent enough to catch a system compromise and react to it before the attacker causes significant damage.

System Log Files. The DIS set up its DEC 8400 system to log significant system events which could have resulted in compromise. However, DIS did not implement system settings to protect the log files from being altered. As a result, a sophisticated intruder could have compromised the system and removed the evidence from the log files before the compromise was discovered. We discuss system security weaknesses in further detail in the Access Controls information.

System Log Reviews. The DIS Information System Security Officer informally reviewed selected extracts from the system logs. However, those procedures were not formalized, continuous, or comprehensive enough to detect a system compromise in progress. As a result, the potential existed for a successful system compromise to occur without the agency having any indication that an attack had taken place.

Access Controls

DIS had serious deficiencies in access controls protecting the DCII database. The DCII resides on a DEC 8400 midtier computer. The operating system used by the DEC 8400 was Digital Equipment Corporations Unix Version 7 (DEC Unix[4]). DEC Unix can be implemented as a C2 compliant product using the DEC "enhanced mode" security, but this feature was turned off. Instead, DIS technical staff had elected to implement DEC Unix as a generic Unix installation. While this made system administration significantly easier, it made security administration to a C2 standard very difficult. Security on the DEC 8400 was implemented far below the C2 level required by DoD 5200.28-STD for systems processing sensitive unclassified information. Security deficiencies existed that could have allowed knowledgeable unauthorized individuals to:

- log onto the system without having a user account;
- copy the DCII database files, or many other files on the system;
- view sensitive system settings without authorization; or
- potentially manipulate the system to gain root, or superuser, access.

The DEC 8400 server was connected to the DIS local and wide area networks. DIS has two other midtier servers, as well as a local area network, a firewall machine, and several unix workstations connected to the same network. We confined our review to

---

[4]DEC Unix is a registered trademark of Digital Equipment Corporation. Generic Unix is a standard operating system that is in the public domain and is implemented on many midtier computer systems. Many versions of generic unix are available at no cost.

the DIS DEC 8400 server and selected features of the DIS local area network architecture. The deficiencies are discussed here in general terms only because of the sensitive nature of the access control deficiencies. We provided the specific details of those deficiencies in discussions with DIS managers. Management agreed with our recommendations and initiated action to correct system security deficiencies during fieldwork.

Network Architecture

DIS needed to improve network architecture to more effectively protect its critical network resources from compromise. The network architecture in place left critical network components vulnerable to attack from DoD employees as well as internet intruders. DIS management has a planned network architecture, to be implemented by November 1997, that partially isolates critical network resources. However, DIS needs to go beyond those plans and further isolate its critical network resources to most effectively protect those systems.

Types of Network Architecture. Network architecture is the physical configuration of the various machines that form a computer network. A network architecture can be designed as "open," which grants full accesses to all network resources. Alternately, a multilevel security architecture can be implemented. A multilevel security architecture isolates critical network resources so they can be protected more cost-effectively.

"Open" Architecture. The most basic network architecture that can be set up is referred to as an "open" architecture. An open architecture grants every resource on a network full access to every other resource. An open architecture is very easy and cost effective to administer from an operational standpoint. From a security standpoint, however, an open architecture is very difficult to administer. The only way to protect the network adequately is to protect every network resource as though it contains the most critical data on the network. This includes such resources as personal computers connected to the network, and even local area network (LAN) equipment and cables. It is almost never cost effective to implement an open network from a security standpoint unless the network does not contain any sensitive data.

"Multilevel Security" Architecture. A more complex network architecture can be established that is referred to as a multilevel security architecture. A multilevel

security architecture isolates critical network resources and prevents less well-protected portions of the network from accessing them without authorization. Different levels of security can be implemented on various parts of the network by isolating critical resources. A multilevel security architecture is more difficult to administer from an operational standpoint, but it makes security administration significantly easier. Because security can be implemented at different levels on various parts of the network, significant savings can be achieved by implementing much lower levels of security on the lower-risk portions of the network.

DIS Network Architecture. The DIS implemented its network using an open architecture. Management has plans to move the DIS network to a multilevel security architecture by November 1997. However, those plans did not isolate critical resources on the DIS network so resources could be cost-effectively protected. DIS could maximize security and minimize costs through implementing a lower level of security on the noncritical portions of the network by isolating the network resources that process its most sensitive data.

Physical Security at DIS Personnel Investigations Center

DIS needed to improve physical security at its Personnel Investigations Center (the Center) in Baltimore, Maryland, to more effectively protect its critical systems and data. Access into the center was not adequately controlled. Sensitive areas of the center, such as the investigations processing area, and telephone and LAN cabling rooms, were not locked to prevent unauthorized entry. Floor plans were displayed at every entrance which gave too much information about LAN cabling and telephone rooms. Finally, badge policies were not enforced even though DIS had policies requiring display of badges by all employees. Because of physical security weaknesses, unauthorized personnel could have entered the center, obtained access to sensitive privacy act information, or stolen valuable computer, LAN or telephone equipment. Further, a sophisticated hacker could have used physical access into the center to circumvent system security and gain access to all DIS automated data.

Access into the DIS Personnel Investigations Center. Security was not sufficient to prevent unauthorized access even though DIS had physical security, including guards and a perimeter fence at its Personnel Investigations Center. The front guard gate, a critical portion of the perimeter security, was not staffed or was staffed only

sporadically. Further, although guards protected the front entrance to the building, the side exits remained unlocked, and unauthorized individuals could gain access to the building through those routes. Also, inadequate badge enforcement policies (discussed below) did not allow center guards to easily identify unauthorized individuals.

Access into Sensitive Areas. The DIS Personnel Investigations Center contained several sensitive facilities that required additional security. Those areas included the computer processing center and the telephone cable rooms. The DIS did not adequately protect the computer processing facility or the telephone cable rooms from unauthorized intrusion.

DIS Computer Center. Intrusion detection devices either were not installed or were not activated in the computer center. The center was regularly unstaffed, although it was kept locked. A computer center should be protected very strongly for two reasons. First, computer equipment is usually very valuable and is a prime target for theft. Second, access to the physical computer equipment, even for a very brief period, would allow an intruder to completely compromise a computer system and install unauthorized software that would grant remote entry to the system at a later time. DIS had no way of determining whether a break-in had occurred because the computer center was unstaffed and intrusion detection devices were not being used.

Telephone Cable Rooms. Telephone cable rooms at the center were not secured from unauthorized entry. The doors to those rooms were unlocked and sometimes left standing open. Telephone cable rooms usually contain all of the telephone connections for a building floor. The cable rooms often house LAN connections and equipment for an organization's computer network. A sophisticated intruder can place a network sniffing device[5] in a telephone cabling room. Telephone cable rooms should be unmarked and secured from unauthorized entry at all times because they present such significant weaknesses.

Floor Plans Displayed. The center posted floor plans at each exit, in each stairwell, and at various places throughout the building to show emergency exit routes. However, those floor plans contained too much information. In addition to required

---

[5]A network sniffing device is a commonly available device that plugs into an ordinary LAN connection and monitors all of the traffic on that network. A sniffing device can be set to capture user names and passwords that are sent over the network.

information, such as exits from the building and emergency routes, floor plans revealed such information as the location of telephone cabling rooms and LAN data conduits. That information could be used by a sophisticated intruder to place network sniffing devices, or by a thief to identify the location of valuable equipment. Emergency route floor plans should be generic, showing only the emergency exits from the buildings, and the preferred route to the nearest exit, to protect center assets.

Badge Policies. DIS badge policies were not enforced at the center. Employees of the center frequently wore their badges improperly displayed, or did not wear them at all. Guards on patrol did not challenge individuals with improperly displayed badges. As a result, guards were unable to easily identify unauthorized individuals. Enforcing badge policies would allow guards to easily identify and challenge unauthorized individuals in the center.

Summary

Although DIS was committed to protecting its critical systems and data, managers had not yet implemented effective controls to ensure adequate security. The weaknesses in the DIS systems were typical of those commonly found in DoD systems, as discussed in numerous other audit reports, GAO reports, and DoD reviews. Specifically, management needed to communicate security policies better and implement enhanced security procedures to protect its systems. While we found no evidence of unauthorized intrusions, there has been and continues to be risk that unauthorized individuals may be able to access, modify, or destroy the highly sensitive DoD personnel security information that DIS administers. Correcting the deficiencies in the DIS systems should be a high priority DoD information assurance goal.

Management Comments on the Finding and Audit Response

Management Comments on the Finding. DIS disagreed with our conclusion that their networks and systems were vulnerable to attack, stating that they had been proactive in protecting their networks. DIS claimed that in a penetration review conducted by the National Security Agency (NSA) in April 1997, NSA had been

unable to penetrate DIS's network, and had found only minor problems. DIS stated that an attack was unlikely because hackers would be deterred by the expense of executing an attack on their network or systems.

Audit Response. We do not agree that the DIS systems have been or are yet adequately protected. Our review of the DIS systems and the NSA security analysis revealed multiple avenues for outside attacks that could be launched against the DIS network. Further, our analysis of the DIS DCII server, the most critical portion of the DIS network, revealed as many as twenty-four different uncorrected weaknesses that could have allowed a relatively unsophisticated outsider to circumvent system security.

We reviewed the NSA report in August and noted that NSA's findings substantially agreed with ours. NSA identified thirteen critical weaknesses in the DIS network that would allow outsiders to successfully attack DIS systems. The NSA conclusion, expressed on page 54 of their report, stated:

> In general the DIS network was found to be vulnerable to attacks through each of its components, either through inherent system vulnerabilities or through misconfiguration problems of the components. The internal network scan also found many vulnerable systems on the DIS intranet.

DIS states that the cost to an attacker attempting to exploit DIS systems would be prohibitively high. Based on our research, we cannot agree with this statement. NSA also emphasized the essential vulnerability of DIS systems by stating that the DIS network could have been successfully compromised, "by the casual hacker . . . using widely published attack scripts."

DIS told us that server weaknesses were corrected September 16, 1997. Correction of critical architecture weaknesses, however, is not scheduled until February 1998. Based on our findings, and on those of the National Security Agency, we believe that the DIS network is vulnerable to attack and will continue to be vulnerable until those critical architecture weaknesses are corrected.

Recommendations and Management Comments

Deleted and Renumbered Recommendations. DIS management concurred with all but one of the 10 recommendations and actions have been initiated to correct the weaknesses identified in the report. DIS did not concur with draft Recommendation 3. to reposition their Information Systems Security Officer to obtain greater autonomy and objectivity. We have deleted draft Recommendation 3., and renumbered subsequent recommendations because DIS management has concluded that the Information System Security Officer was appropriately placed in their management structure. Management comments were responsive to the recommendations.

We recommend that the Director, Defense Investigative Service:

1. Develop and implement a Trusted Facility Manual that communicates the specific intended level of security, the specific resources that should be protected, and the specific technical functions that should be controlled on the Defense Investigative Service computer network.

Management Comments. The Defense Investigative Service concurred and stated that a detailed Trusted Facility Manual would be made available to systems administrators by November 30, 1997.

2. Modify all current and future memorandums of agreement that provide other organizations access to Defense Investigative Service network resources. Those memorandums of agreement should stipulate the level of security that organizations should maintain over Defense Investigative Service resources to which they have access, identify procedures for security monitoring on the part of the Defense Investigative Service, and contain provisions to disconnect service if the organizations fail to maintain adequate security.

Management Comments. The Defense Investigative Service concurred and stated that Memorandums of Agreement would be updated regularly starting October 1, 1997.

3. Develop and implement an access control policy, including documented security procedures, to periodically ensure that system security is implemented to the appropriate level, maintain a baseline of critical system settings to guard against unauthorized changes, and monitor Defense Investigative Service systems to detect and react to attacks and compromises.

Management Comments. The Defense Investigative Service concurred and plans to implement documented security procedures by December 1, 1997.

4. Implement system security on critical portions of the Defense Investigative Service computer systems and network to the C2 level as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, and DoD Standard 5200.28, DoD Trusted System Evaluation Criteria," December 26, 1985, to include identifying and protecting critical network resources from unauthorized access, modification, or destruction.

Management Comments. The Defense Investigative Service concurred in principle and stated that C2-like controls were implemented on critical portions of the DIS network by October 17, 1997.

5. Implement a network architecture that isolates critical network resources and allows for more cost-effective protection of those resources.

Management Comments. The Defense Investigative Service concurred and plans to implement a segmented, isolated network architecture, including the removal of the communications line bypassing their network firewall, by February 1, 1998.

6. Improve physical security at the Defense Investigative Service Personnel Investigations Center in Baltimore, Maryland, to preclude physical access by unauthorized individuals.

Management Comments. The Defense Investigative Service concurred and stated that physical security at the Defense Investigative Service was upgraded on September 2, 1997.

7. Secure the Defense Investigative Service computer center using intrusion detection devices to detect unauthorized access.

Management Comments. The Defense Investigative Service concurred and plans to secure the computer center by December 1, 1997.

8. Physically secure telephone cable rooms at the Defense Investigative Service Personnel Investigations Center in Baltimore, Maryland, to protect the Defense Investigative Service network from compromise.

Management Comments. The Defense Investigative Service concurred and plans to physically secure all telephone cable rooms by February 1, 1998.

9. Enforce the Defense Investigative Service badge policy to ensure that facility guards at the Personnel Investigations Center in Baltimore, Maryland, are able to identify unauthorized individuals.

Management Comments. The Defense Investigative Service concurred and states that badge policies have been strictly enforced since September 1997.

THIS PAGE INTENTIONALLY LEFT BLANK

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

We reviewed security controls over selected systems and networks administered by the Defense Investigative Service. We also reviewed compliance with DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, and DoD Standard 5200.28, "DoD Trusted Computer System Evaluation Criteria," December 26, 1985.

Use of Computer-Processed Data. We used standard utility programs and reports generated by commercial operating system software to satisfy our objective on computer system security. To assess security rules, features, and administration, we used data generated by the Unix operating system implemented by DIS on its computer systems. All system testing and data extraction were done in a controlled environment with management's approval. Based on those tests, we concluded that data we found were sufficiently reliable to meet the audit objectives and support our audit conclusions.

Audit Type, Dates, and Standards. We performed this program audit from April through August 1997 in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. We did not use statistical sampling procedures to conduct this audit. We included tests of management controls that we considered necessary. We conducted all of our audit work at the Defense Investigations Service, Personnel Investigations Center in Baltimore, Maryland.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Management Control (MC) Program," and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," dated August 26, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of the Management Control Program. We reviewed the adequacy of selected management controls ensuring the confidentiality, reliability, and integrity of data processed on DIS computer systems and networks. We reviewed the DIS Annual Statement of Assurance for FY 1996 and the implementation of the DIS Directorate for Information Services management control program.

Adequacy of Management Controls. We identified materiel management control weaknesses at the Department level, as defined by DoD Directive 5010.38, relating to computer security at DIS. Weaknesses in computer security at DIS threatened the confidentiality and integrity of highly sensitive DoD personnel security information for over 15 million individuals. Recommendations 1-5, and 7, if implemented, will correct this problem. A copy of this report will be provided to the senior official responsible for management controls in the Defense Investigative Service, in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and in the Office of the Secretary of Defense.

Adequacy of Management's Self-Evaluation. DIS identified security over its computer systems and networks as part of an assessable unit and, in our opinion, correctly identified the risk associated with computer security as high. However, DIS management's self-evaluation was not adequate because it did not identify the specific management control weaknesses identified by this audit. Management did not identify those weaknesses because of communication problems discussed in Part I of this report.

Appendix B. Summary of Prior Coverage

General Accounting Office

GAO Report No. AIMD-96-144 (OSD Case No. 1213), "DoD General Computer Controls: Critical Need to Greatly Strengthen Computer Security Program," September 30, 1996. The report discusses GAO's evaluation of the general computer controls at several large Navy and Marine Corps computer installations and at selected DISA Defense Megacenters. The report notes security weaknesses that would allow hackers and legitimate users privileges to improperly access, modify, or destroy sensitive DoD Data. The report recommended a centralized security management program with defined responsibilities, periodic reviews, and monitoring and reporting of improvement actions. DoD management concurred with all findings and recommendations.

GAO Report No. AIMD-96-84 (OSD Case No. 1150), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996. The report discusses GAO's review of the extent to which DoD computers are being attacked, the potential for damage, and the challenges faced in responding to those attacks. GAO notes that attacks are increasing and damaging, and are a threat to national security. GAO concludes that policies are out-of-date and inconsistent, and that many users are not aware of the magnitude of the problem. The report recommended that the Secretary of Defense strengthen the DoD information systems security program by improving policies and procedures, increasing user awareness, setting standards, monitoring security, and establishing responsibility and accountability. DoD management agreed with the report findings and recommendations.

Office of the Inspector General, DoD

Report No. 97-196, "Personnel Security in the Department of Defense," July 25, 1997. The audit objective was to determine the effectiveness and efficiency of the management of the DoD personnel security program. The report concludes that the management of the DoD personnel security program is improving as a result of extensive process re-engineering. The report contains no recommendations.

Other Related Coverage

Defense Science Board Task Force, "Information Warfare-Defense (IW-D)," November 21, 1996. The task force was established to study the protection of information interests of national importance through a credible information warfare defensive capability. The report concludes that action is needed to defend against possible information warfare attacks against DoD systems that could impact the ability of DoD to carry out its responsibilities. The Task Force recommended 50 actions ranging from identification of a focal point within DoD for IW activities, to allocation of approximately $3 billion over the next five years to implement recommendations.

Joint Security Commission, "Redefining Security," February 28, 1994. The Joint Security Commission report addresses the processes used to formulate and implement security policies in the DoD and the intelligence community. The Joint Security Commission concluded that the clearance process is needlessly complex, cumbersome, and costly. The Joint Security Commission made recommendations that would create a new policy structure, enhance security, and lower cost by avoiding duplication and increasing efficiency. The President issued Executive Order 12968 in response to the Commission report.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director for Information Assurance
Assistant Secretary of Defense (Personnel & Security)
Assistant Secretary of Defense (Public Affairs)
Director, Administration and Management

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Army Logistics Management College
  Director, Defense Logistics Studies Information Exchange

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Superintendent, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Air Force Audit Agency

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Director, Defense Investigative Service
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  National Security Division, Special Projects Branch
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Non-Defense Federal Organizations and Individuals (cont'd)

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Subcommittee on Personnel, Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security
House Subcommittee on Military Personnel, Committee on National Security
House Permanent Select Committee on Intelligence

Part III - Management Comments

Defense Investigative Service Comments

DEFENSE INVESTIGATIVE SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

OCT 31 1997

MEMORANDUM FOR SECRETARY OF DEFENSE
DEPUTY SECRETARY OF DEFENSE
INSPECTOR GENERAL, DOD

SUBJECT: Audit on Security Controls Over Systems Serving the DoD Personnel Security Program

Reference the Department of Defense Inspector General's, Information Memorandum, dated August 26, 1997, regarding subject as above. The Defense Investigative Service (DIS) has addressed each of the audit's recommendations for corrective action. The audit is based on a specific point in time, thus it does not reflect an accurate picture of our overall security posture. Also contrary to the audit, the sole implementation of the recommendations will not protect the critical information systems (IS) in question. The information provided in this response demonstrates that DIS has been proactive in its IS security posture. DIS therefore does not agree with the audit report's conclusion that DIS had not communicated security policies nor implemented procedures to ensure the protection of critical systems.

DIS began a year ago, an ongoing aggressive IS security program to enhance the security of its new systems and networks. This included the implementation of strong identification and authentication for access to certain critical information. The National Security Agency was enlisted to conduct extensive vulnerability testing on DIS's networks and systems. The Defense Information Systems Agency recently performed live vulnerability assessment penetrations on our systems and networks to confirm that all previously identified weaknesses were corrected. We implemented a dynamic Agency-wide security awareness program to include a mandatory briefing for all agency employees.

Since any information system is vulnerable to exploitation of some type, be it for destruction of data, denial of service or other motivations, security countermeasures must be measured in terms of the cost that an attacker must expend to successfully exploit the system versus the value of the information being exploited. By virtue of our ongoing initiatives in the implementing of counter-measures relative to other Sensitive But Unclassified (SBU) systems, the cost to an attacker attempting to exploit DIS systems would be substantially high. This fundamental precept was not addressed in the audit; therefore, DIS cannot agree with the conclusion being drawn.

DIS has an aggressive IS program of security initiatives to eliminate vulnerabilities. Moreover, we believe the Agency has initiated one of the strongest security programs within the DoD for protecting SBU information.

Margaret R. Munson

MARGARET R. MUNSON
Director

Attachment

Defense Investigative Service (DIS) Responses to Inspector General, DoD, Proposed Audit 6RD-5094.02 Recommendations

DIS responses to the DoD Inspector General's (IG) Recommendations for Corrective Action are addressed as follows:

Recommendation 1: Develop and implement a Trusted Facilities Manual that communicates the specific intended level of security, the specific resources that should be protected, and the specific technical functions that should be controlled on the Defense Investigative Service computer network.

Response:

- The DIS Information Systems Security Office (ISSO) had developed a "DEC UNIX Security Review" document. This document identifies UNIX Operating System security risks and vulnerabilities; and management of the same. This document was provided to all DIS system administrators.
  Completed - April 1997

- However, based on a recommendation by the DoDIG, the ISSO is reviewing the Defense Information Systems Agency (DISA), Western Hemisphere, "UNIX Security Technical Implementation Guide, Version 1, Release 2" for DIS adaptation. The new document will also include all other DIS operating systems.
  Target Date - November 30, 1997

- DIS has developed and is implementing a computer security awareness program which includes an annual computer security awareness briefing. This includes a presentation of Federal and DoD security policies; handouts of the "DIS Internet Security Policy," (draft-September 1997) and the DIS "Security Policy on the Use of Microcomputers and Peripherals for Processing Classified Data," (dated June 1997); and each attendee is required to sign a Security Awareness Agreement acknowledging they understand and will comply with DIS security policy.
  Target Date - April 2, 1998

Recommendation 2: Modify all current and future memorandums of agreement that provide access to Defense Investigative Service network resources to stipulate the level of security that organizations should maintain over Defense Investigative Service resources to which they have access and to contain provisions for security monitoring on the part of the Defense Investigative Service and disconnection of service if the organizations fail to maintain adequate security.

Response

- The security protection procedures implemented for DIS resources are reviewed and approved by the Designated Approving Authority (DAA). The DAA is the Agency's Chief Operating Officer.

Defense Investigative Service Comments

ıal Report Reference

- DIS transferred the responsibility for the execution of Memorandums of Agreement (MAO) from the Information Services Directorate (ISD) to the DIS Headquarters Policy Directorate.
  Completed - October 1, 1997

- The DIS Policy Directorate will ensure that the Memorandums of Agreement (MOAs) contain provisions stipulating the level of security the organizations should maintain over their DCII connections. DIS is developing security monitoring provisions which will be incorporated into the MOAs. These provisions include the requirement for Smartgate tokens to accomplish access through a firewall, and DIS' ability to discontinue the service if the organization fails to meet the security provisions. In the case of the pending connection with the Office of personnel Management, the MOA modifications that include the security provisions is in coordination.
  Target Date - Ongoing

Deleted

Recommendation 3: Restructure the Defense Investigative Service so that the Information Systems Security Officer has the authority and autonomy necessary to adequately perform assigned duties.

Response:

- DIS disagrees with the assumption requiring this recommendation. It is DIS' assertion the position currently has all of the organizational objectivity and authority required to implement a viable security architecture.

umbered as Recommen-dation 3.

Recommendation 4: Develop and implement an access control policy, including documented security procedures to periodically ensure that system security is implemented to the appropriate level, maintain a baseline of critical system settings to guard against unauthorized changes, and monitor Defense Investigative Service systems to detect and react to attacks and compromises.

Response:

- The ISSO has submitted an "Internet Security Policy" to the Director, DIS for signature. This policy was developed with the concept that the majority of DIS system access to the Internet would be via DISA's Non-Classified Internet Protocol Router Network (NIPRNET). This policy has been coordinated with the National Security Agency (NSA). The policy provides guidance to DIS information systems (IS) users in the use and protection of IS connected to the NIPRNET. The DIS policy also identifies security roles and responsibilities for the IS users, system and network administrators, and technical support personnel. It provides guidelines and procedures for configuration and implementation of information systems security controls and countermeasures for the DIS IS.
  Target Date - November 17, 1997

- IS administrators received training on the installation and management of Computer Associate's CA-Unicenter software security package. This package establishes system

Final Report Reference

security baselines, assists in the detection of critical changes to system settings, and provides on-going monitoring. The package will allow systems administrators to ensure the integrity, accuracy, privacy and confidentiality of DIS data and programs.
Target Date - December 1, 1997

- Digital Equipment Corporation's Enhanced UNIX Security was installed on DIS 8400 database servers in September 16, 1997. This enhanced security version of UNIX protects DIS password file with encryption. The operating system's features allows DIS to disable users after three successive login failures, and allows systems administrators to limit access permission to DIS Sensitive But Unclassified (SBU) information.
Completed - September 16, 1997

- DIS coordinated with NSA to conduct vulnerability testing. NSA was unable to penetrate our systems. NSA did identify some weaknesses which have been corrected.
Completed - May 1997

- DIS and NSA have initiated an agency-wide security architecture review, and executed an agreement for future penetration testing.
Target Date - Ongoing

- The Defense Information Systems Agency has performed live vulnerability assessment penetrations (VAP) on our systems and networks to confirm that all weaknesses were corrected.
Completed - October 10, 1997

- DIS and DISA have implemented a program of periodic real-time unannounced VAP testing at strategic locations throughout the Agency.
Target Date - Ongoing

- DIS is staffing an organizational level configuration management (CM) program with two experts and a supporting staff, to ensure that any software or hardware changes do not adversely impact systems or security processes.
Target Date - November 28, 1997

Recommendation 5: Implement system security on Defense Investigative Service computer systems and network to C2 level as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988, and DoD Standard 5200.28, DoD Trusted System Evaluation Criteria," December 26, 1985, to include identifying and protecting critical network resources from unauthorized access, modification, or destruction.

Renumbered a: Recommendation 4.

Response:

- C2 level security was designed for stand alone systems. DIS has implemented C2-like security controls which include identification and authentication, encryption, auditing, monitoring, documentation, and security testing. DIS has applied a V-One IS security

Final Report Reference

methodology to include a firewall and client-server programs to promote strong identification and authentication, and encryption. We also use Secret Agent. This encrypts files on desktop and notebook computers.
Completed - October 17, 1997

enumbered as Recommendation 5.

Recommendation 6: Implement a network architecture that isolates critical network resources and allows for more cost-effective protection of those resources.

Response:

- DIS is segmenting its Local Area Network (LAN). The network architecture is being changed so that all internal users must authenticate through a firewall for access to critical I information , as well as to the LAN and application, i.e. DCII. Further the DIS Database Administrator implements and restricts the user's levels of access. The eligibility determination for a user's access is based upon the employee's job description and responsibilities, requiring approval by their supervisor. Additionally the Terminal Area Security Officer monitors employee adherence to approved established policies and practices.
  Target Date - February 1, 1998

Renumbered as Recommendation 6.

Recommendation 7: Improve physical security at the Defense Investigative Service Personnel Investigations Center in Baltimore, Maryland, to protect the Center from physical access by unauthorized individuals.

Response:

- DIS has staffed the guardpost at the entrance of the DIS perimeter. Positive identification of all vehicles and individuals is accomplished upon entry. All opened entrances are controlled by a federally employed, qualified guard.
  Completed - September 2, 1997

Renumbered as Recommendation 7.

Recommendation 8: Secure the Defense Investigative Service computer center using intrusion detection devices to detect unauthorized access.

Response:

- An intrusion alarm will be installed on the door to the computer room and will be monitored at the guard station.
  Target Date - December 1, 1997

Renumbered as Recommendation 8.

Recommendation 9: Physically secure telephone cable rooms at the Defense Investigative Service Personnel Investigations Center in Baltimore, Maryland, to protect the Defense Investigative Service network from compromise.

Final Report Reference

Response:

- All telephone cable rooms are now locked except for two rooms which do not have adequate air conditioning. These rooms remain open to allow for better ventilation. DIS has requested that the Army Corps of Engineers provide a cooling solution for these two rooms. We have implemented procedures controlling the issuance of these room. All emergency route floor plans posted have been modified to eliminate any reference to cable rooms.
  Target Date - February 1, 1998

Recommendation 10: Enforce the Defense Investigative Service badge policies to ensure that facility guards at the Personnel Investigations Center in Baltimore, Maryland, are able to identify unauthorized individuals in the Center.

Renumbered as Recommendation 9.

Response:

- The guard force is aggressively enforcing the DIS badge policy by controlling the building access and challenging individuals not displaying their badges.
  Completed - September 1997

Audit Team Members

This report was prepared by the Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD

Thomas F. Gimble
Salvatore D. Guli
Robert M. Murrell
Mary L. Ugone
Judith I. Padgett
J. David Stockard
Michael Carlson

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Security Controls Over Systems Serving The DOD Personnel Security Program

B. DATE Report Downloaded From the Internet: 09/28/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/28/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.