Audit Report

OFFICE OF THE INSPECTOR GENERAL

SECURITY OVER NETWORKS USED TO TRANSMIT U.S. SPECIAL OPERATIONS COMMAND FINANCIAL DATA

Report No. 97-216

September 18, 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 to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CIO	Chief Information Officer
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
IP	Internet Protocol
LAN	Local Area Network
NIPRNET	Not Classified Internet Protocol Router Network
SNA	Systems Network Architecture
SOCOM	U.S. Special Operations Command

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

September 18, 1997

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. SPECIAL OPERATIONS COMMAND
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on Security Over Networks Used to Transmit U.S. Special Operations Command Financial Data (Report No. 97-216)

We are providing this report for information and use. We performed this audit in response to the Chief Financial Officers Act of 1990 and the Federal Financial Management Act of 1994. We considered management comments on a draft of this report in preparing the final report.

Management comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone, Audit Program Director, at (703) 604-9426 (DSN 664-9426) or Ms. Cecelia A. Miggins, Audit Project Manager, at (703) 604-9436 (DSN 664-9436). See Appendix F for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 97-216 **September 18, 1997**
(Project No. 6RE-2031)

Security Over Networks Used to Transmit U.S. Special Operations Command Financial Data

Executive Summary

Introduction. In April 1987, the U.S. Special Operations Command was established to unify the special operations forces and is composed of four subordinate commands. The U.S. Special Operations Command has 103 organizations that access at least 20 financial applications processing their financial data. The Defense Finance and Accounting Service owns the financial applications, while the Defense Information Systems Agency operates the 16 Defense megacenters where the applications are processed.

The DoD Annual Statement of Assurance for FY 1996 identifies information systems security as a systemic weakness within the DoD. Increases in computer systems intrusions have highlighted the vulnerability of unclassified systems and networks providing support and sustainment functions to information-warfare type attacks.

Audit Objective. The audit objective was to evaluate the financial systems supporting the U.S. Special Operations Command FY 1996 financial statements and the effect of any noncompliance on the FY 1997 financial statements. Specifically, we evaluated the adequacy of information assurance over the financial systems to ensure the confidentiality, integrity, and availability of the financial data.

Audit Results. The U.S. Special Operations Command has no assurance that its financial information, which is transmitted and processed through several financial applications and networks, is secured against compromise. As a result, the U.S. Special Operations Command financial data that support the DoD consolidated financial statements for FY 1996 and subsequent years may not be reliable.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Special Operations Command, conduct a risk analysis of the 103 organizations' networks and of their entry points to other networks and obtain memorandums of agreement for safeguarding the financial systems with the designated approval authorities for networks to which the U.S. Special Operations Command is connected.

Management Comments. The Commander in Chief, U.S. Special Operations Command, concurred with the recommendations. The U.S. Special Operations Command plans to conduct risk assessments of its unclassified systems that access financial data, identify the designated approval authority for the applicable connected computer networks, and enter into a memorandum of agreement that specifies the security responsibilities for those interconnected computer networks. See Part I for a complete discussion of management comments and Part III for the complete text of the management comments.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objective 4
Security of the Networks Used to Transmit U.S. Special Operations Command Financial Data 5

Part II - Additional Information

Appendix A. Audit Process
Scope and Methodology 18
Audit Period, Standards, Locations, and Contacts 19
Appendix B. Prior Audits and Other Reviews 20
Appendix C. List of Defense Finance and Accounting Service Locations 25
Appendix D. Financial Applications Used to Process U.S. Special Operations Command Financial Data 27
Appendix E. Defense Megacenter Locations 29
Appendix F. Report Distribution 30

Part III - Management Comments

U.S. Special Operations Command Comments 34

Part I - Audit Results

Audit Background

Public Law 101-576, "The Chief Financial Officers Act of 1990," established requirements for Federal organizations to submit audited financial statements to the Director, Office of Management and Budget. Public Law 103-356, "Federal Financial Management Act of 1994," significantly expanded the audit requirements established in the Chief Financial Officers Act by requiring the Inspectors General to audit consolidated financial statements covering all accounts and activities for FY 1996 and each succeeding year.

The consolidated DoD financial statement includes a reporting entity entitled "Other Defense Organizations," which includes financial information for the Department 97 appropriation. The Department 97 appropriation is the Office of the Secretary of Defense general fund appropriation allocated to 29 Defense organizations, including the U.S. Special Operations Command (SOCOM). In FY 1996, SOCOM received $2.07 billion in Department 97 appropriations.

U.S. Special Operations Command. The SOCOM was established in April 1987 to unify the special operations forces. The SOCOM is composed of four subordinate commands:

- the Army Special Operations Command, Fort Bragg, North Carolina;
- the Naval Special Warfare Command, Coronado, California;
- the Air Force Special Operations Command, Hurlburt Field, Florida; and
- the Joint Special Operations Command, Fort Bragg, North Carolina.

Headquarters, SOCOM, and its four subordinate commands have a total of 103 organizations that receive Department 97 appropriations from SOCOM.

Major Forces Program 11. Congress established the budget category Major Forces Program 11 for all funds appropriated for special operations programs. Major Forces Program-11 includes funds for operations and maintenance, research and development, procurement, and military construction. The William H. Taft memorandum, "CINCSOC [Commander in Chief, Special Operations Command] Program/Budget," January 24, 1989, made the Commander in Chief,

SOCOM, responsible for the program and budget development and budget execution for Major Forces Program-11 funds. On December 1, 1989, the Deputy Secretary of Defense issued a memorandum, "Guidance for Developing and Implementing Special Operations Forces Program and Budget," that requires SOCOM to continue to use existing Service procedures and processes to execute the Major Forces Program-11 programs. The Defense Finance and Accounting Service (DFAS) provides accounting support for SOCOM.

Defense Finance and Accounting Service. The DFAS is the single DoD organization responsible for finance and accounting procedures, systems, and operations. The DFAS consists of 5 centers, 21 operating locations, and 102 Defense accounting offices.[1] Appendix C lists the DFAS centers and operating locations. When DFAS was established, it assumed ownership of the Services' major financial applications, and it still uses several systems to process SOCOM financial data.

Financial Systems Used to Process SOCOM Financial Data. The DFAS processes SOCOM financial data on DFAS financial applications that are Service unique. The U.S. Army Special Operations Command uses at least eight applications, the Naval Special Warfare Command uses at least five applications, and the Air Force Special Operations Command uses at least nine applications to process the financial and accounting information. Appendix D lists the financial applications used to process SOCOM data. Most of the financial systems reside on mainframe computers at the Defense megacenters.

Defense Megacenters in the Defense Information Systems Agency Western Hemisphere. The Defense Information Systems Agency (DISA) Western Hemisphere manages the 16 Defense megacenters (see Appendix E) that provide centralized information processing to DoD customers. DoD financial applications

[1]DFAS had 102 Defense accounting offices as of September 1996. DFAS is consolidating the Defense accounting offices into the 21 operating locations. By FY 1999, all the Defense accounting offices should be closed and all accounting services will be provided by the 5 centers and 21 operating locations.

and data are processed at each of the 16 Defense megacenters. The SOCOM, DFAS, and DISA could not identify all the specific Defense megacenters that process SOCOM financial data.

DoD Annual Statement of Assurance for FY 1996. The DoD Annual Statement of Assurance for FY 1996 identifies a systemic weakness in information systems security. The Annual Statement of Assurance states that increases in computer system intrusions have highlighted the vulnerability of unclassified information systems supporting finance, logistics, medical, procurement, personnel, research and development activities, and other support and sustainment functions. The DoD is implementing several security initiatives to prevent unauthorized access to Defense networks, systems, and data. The security initiatives include establishing an Information Career Management Program and information security training programs; revising DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988; and improving the security at Defense megacenters.

The 103 SOCOM organizations have access to the financial data processed by 128 accounting offices that use at least 20 financial applications at 16 Defense megacenters. Therefore, the involvement of SOCOM, DFAS, and DISA in securing access to the processing, transmission, and storage of financial data is essential.

Audit Objective

The audit objective was to evaluate the financial systems supporting the SOCOM FY 1996 financial statements and the effect of any noncompliant actions on the FY 1997 financial statements. Specifically, we evaluated the adequacy of the information assurance over the financial systems in ensuring the confidentiality, integrity, and availability of the financial data. Appendix A provides details on the scope and methodology of the audit, and Appendix B summaries prior audit coverage. Management controls are to be reviewed in a future audit.

Security of the Networks Used to Transmit U.S. Special Operations Command Financial Data

The SOCOM has no assurance that its financial information, which is transmitted and processed through several financial applications and networks, is secured against compromise.

Assurance is lacking because SOCOM has not conducted the required risk analysis for its 103 organizations to identify the threats and vulnerabilities to their network entry points used to access financial applications. Also, SOCOM has not established security measures related to accessing computer systems and financial applications.

As a result, SOCOM financial information that supports the DoD consolidated financial statements for FY 1996 and subsequent years may be unreliable for reporting purposes.

Requirement for Risk Analysis

DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, and SOCOM Manual M380-3 "Security: Automated Information Systems Manual," May 4, 1994, require that sensitive, unclassified information be safeguarded to ensure confidentiality, integrity, and availability. DoD and SOCOM guidance also requires that networks be accredited. An accreditation is an approval to operate in a particular security mode using prescribed safeguards. Part of the accreditation process is the performance of a risk analysis. A risk analysis is the process of identifying threats and vulnerabilities and categorizing the level of risk associated with each. DoD Directive 5200.28 also requires that when information systems or networks are interconnected, the

designated approval authorities[2] enter into a memorandum of agreement that identifies the responsibilities for safeguarding the systems. A risk analysis of all the networks requires analyzing the methods used to access financial applications. Several methods and networks are used for accessing data and financial applications. Three commonly used methods are discussed in the following section.

Methods Used to Access the Financial Applications

Authorized users employ three primary methods to access the financial applications run at the Defense megacenters: dial-up, Internet Protocol[3] (IP), and Systems Network Architecture[4] (SNA). Authorized users may also access a Defense megacenter using manual methods, such as tapes and disks.

Dial-Up. With dial-up access, the user accesses the financial applications through a telephone line and a modem. The modem converts the digital signal to an analog signal, which is carried across the public switched telephone network to the modem of the destination computer. Commercial telephone companies, such as AT&T, MCI Telecommunications Corporation, and Sprint, control the telephone lines for the public switched telephone network. Figure 1 illustrates dial-up access.

---

[2]A designated approval authority is the official who has the authority to decide on accepting the security safeguards prescribed for an automated information system and is responsible for issuing the accreditation statement.

[3]Internet Protocol is a communications standard that determines how data will be transferred between two automated information systems.

[4]Systems Network Architecture is a conceptual framework, developed by International Business Machines, that defines communications interactions of an automated information system.

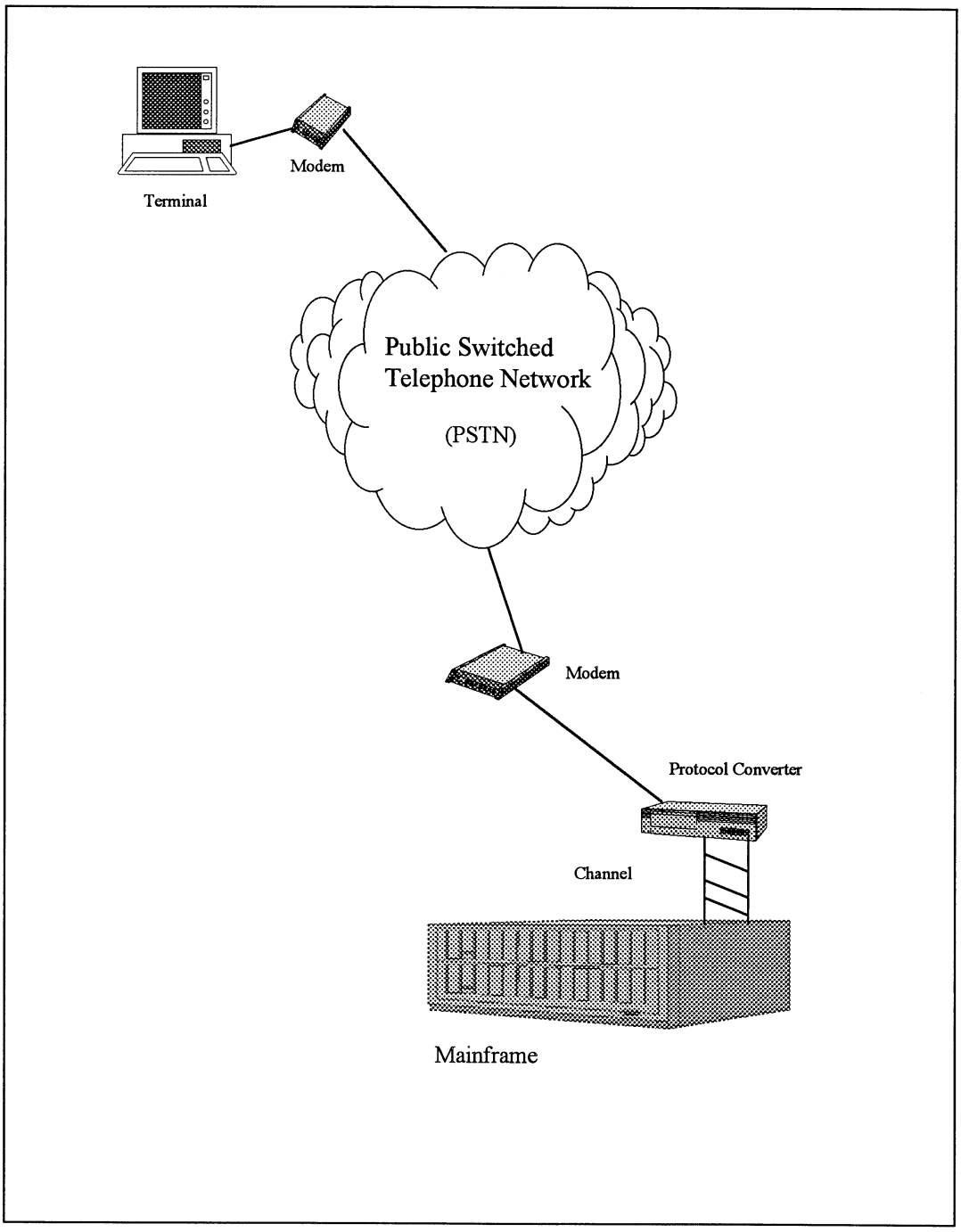

Figure 1. Dial-Up Access Method

Internet Protocol. In using the IP method, data are transferred across combinations of local area networks (LANs),[5] metropolitan area networks,[6] and wide-area networks.[7] Most DoD organizations that use the IP method access the financial applications using the Not Classified Internet Protocol Router Network (NIPRNET).

The IP determines how to send each packet of information based on the IP address of the destination computer. The IP address is a unique decimal number, assigned to each computer, that identifies both the network and the host computer. When the IP address and IP standards are used, routers[8] select a path across the NIPRNET. When a high volume of traffic is on the network, two packages going to the same IP address may be sent along two different routes. Figure 2 illustrates the IP access method.

[5]A LAN is a short-distance data communications network used to link computers and peripheral devices under some form of standard control.

[6]A metropolitan area network is a group of interconnected LANs confined to a specific geographic region. For example, a military base may have a metropolitan area network linking all LANs on the base.

[7]A wide-area network is a group of interconnected LANs covering a large geographic region.

[8]A router is a device used to connect two networks together so that users can transmit data between the two networks.

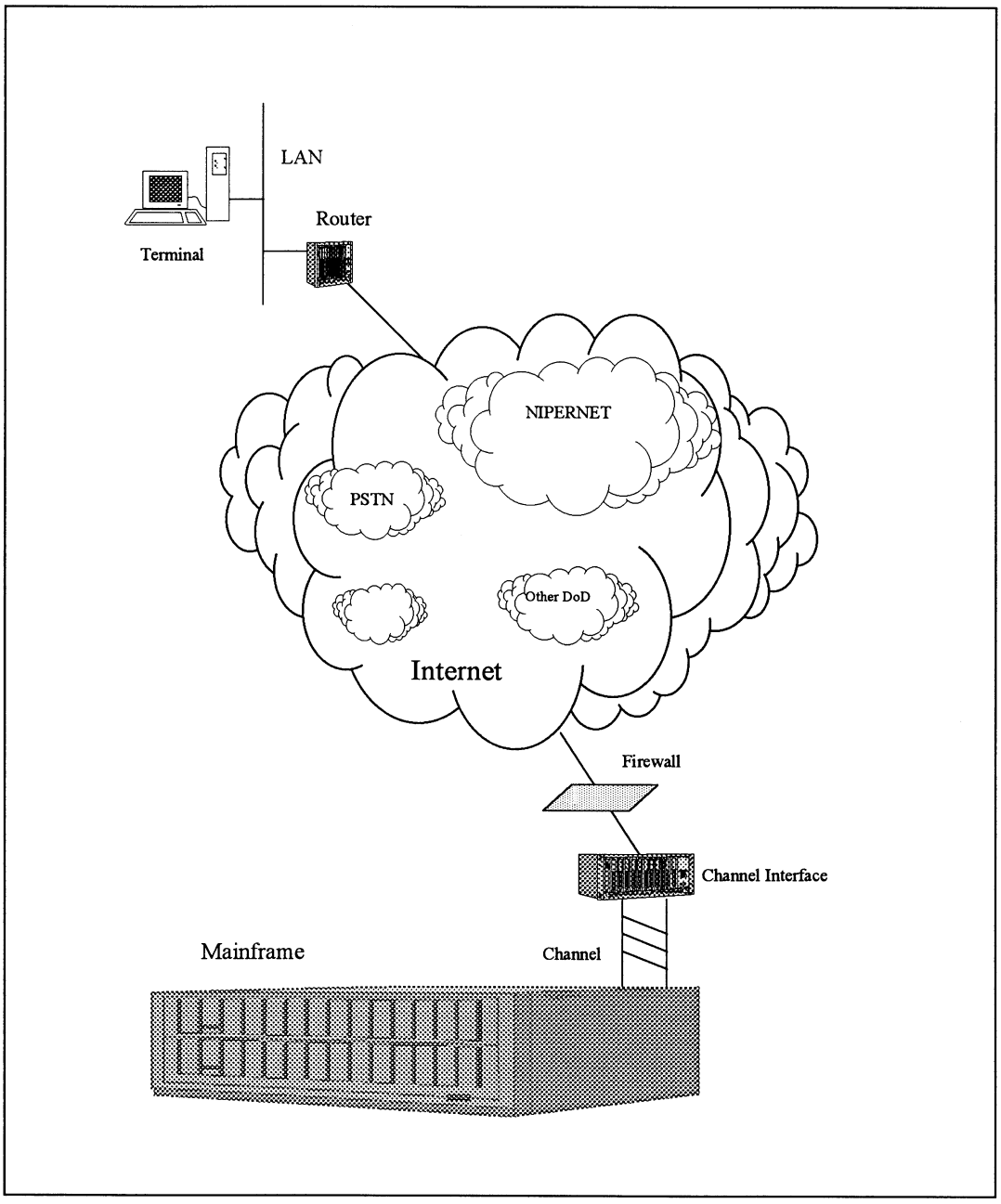

Figure 2. Internet Protocol Access Method

Systems Network Architecture. SNA involves front-end[9] to front-end connectivity using dedicated communication lines. The computer system owner controls access to the dedicated lines. A cluster controller[10] connects remote terminals to the front-end processor. A user must be directly connected to the SNA network to access the specific financial application. Most DoD organizations are migrating from SNA to IP. We were not able to identify any SOCOM or DFAS organizations that use SNA. Figure 3 illustrates the SNA access method.

[9]A front-end processor is an auxiliary processor between the computer central processor and the communications devices to handle functions such as circuit management and code translation.

[10]A cluster controller controls input and output operations of devices, such as microcomputers, printers, scanners, and terminals, that are connected to it.

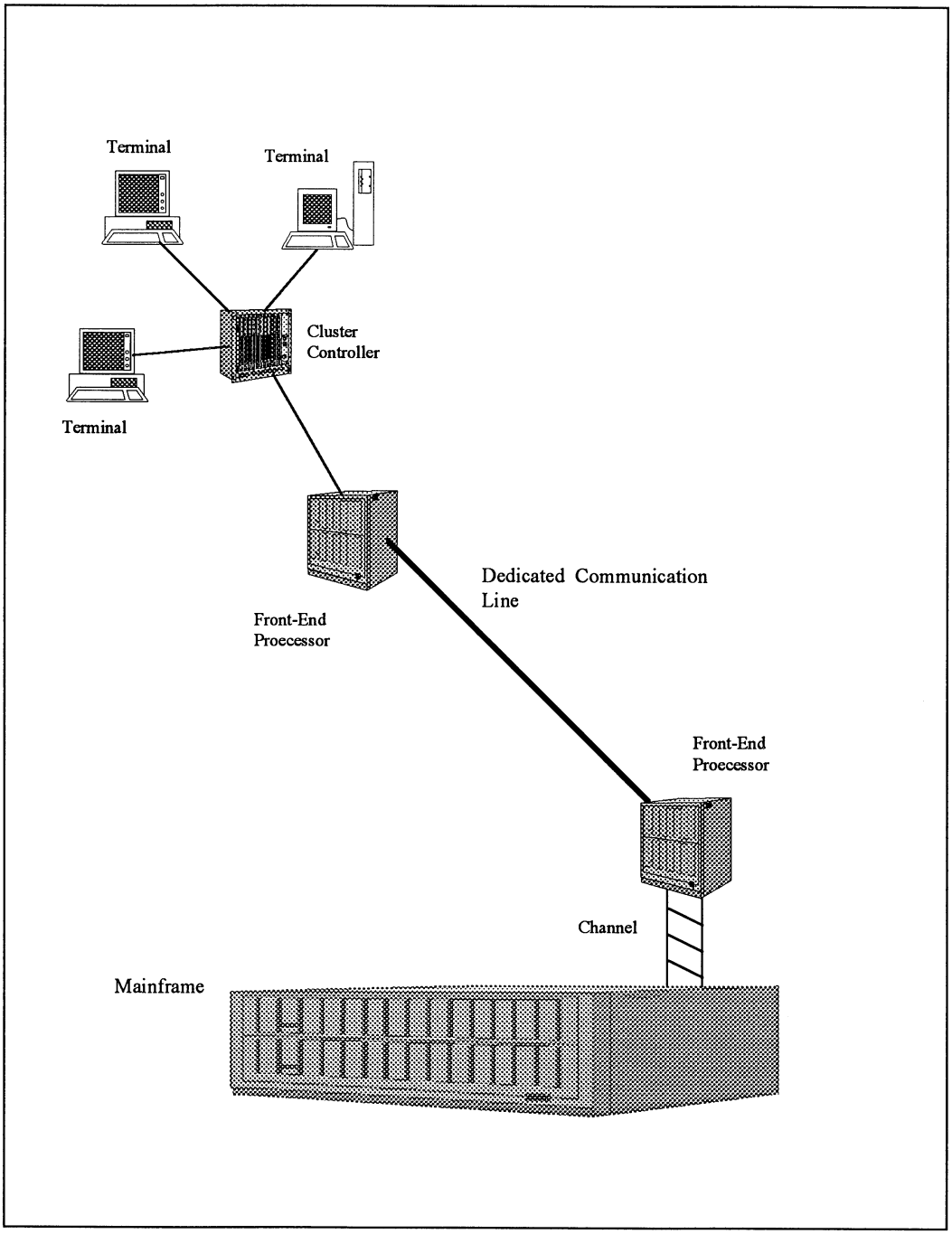

Figure 3. Systems Network Architecture Access Method

Security Measures and Devices. To protect financial applications and data from unauthorized access or compromise, DoD Directive 5200.28 requires SOCOM, DFAS, and DISA to implement security measures that control access to networks from their respective entry points. Types of security measures are dependent on the method used to access the financial application and data.

Protection of Dial-Up Access. Modem entry points are vulnerable to unauthorized access if not properly protected. One security device used to protect a modem entry point is a dial-up security challenge application, which provides a "challenge" to the user before allowing access. The challenge may consist of the user entering a password that is separate from the logon password. Another security device used to protect dial-up entry points is a dial-back modem. A dial-back modem logs the phone number of the modem that the user is calling from, then compares the number to a list of authorized numbers. If the number is authorized, the modem dials back the user's modem and grants access.

Protection of Internet Protocol Access. An IP entry point is a significant vulnerability if not properly protected. One of the most commonly used security devices is the firewall. A firewall is a router, gateway, or computer that filters information going in and out of a network. The firewall blocks access to unauthorized users. However, to be effective, all access must go through the firewall. Therefore, the IP access has to have either a single entry point or a firewall at each entry point used for IP access. Both DISA and DFAS are installing firewalls to protect their IP entry points.

Protection of Systems Network Architecture. The SNA method of access is considered to be more secure than the IP method. The SNA method is considered more secure because the user must be directly connected to the SNA network to gain access. However, SOCOM organizations must implement some security measures to prevent an unauthorized user from connecting directly to the SNA network. With the migration from SNA to IP, the emphasis on security for the SNA has lessened.

Responsibilities for Information Assurance

SOCOM, DFAS, and DISA all have specific responsibilities in safeguarding the SOCOM financial data. All three organizations must fulfill their responsibilities to achieve information assurance.

SOCOM Responsibilities. SOCOM is responsible for information assurance over the entry points to the networks that SOCOM personnel use to access the financial applications. For example, if a SOCOM user accesses a financial application using IP from a SOCOM LAN, SOCOM is responsible for information assurance for the SOCOM LAN up to the point at which the LAN connects to the NIPRNET. Other organizations are responsible for the information assurance for the other segments, such as the mainframe computer and financial application.

DFAS Responsibilities. As the owner and user of DoD financial applications, DFAS has two areas of responsibility. First, DFAS must safeguard the entry points to the networks that DFAS personnel use to access the financial applications. For example, if a DFAS user is accessing the financial application using IP from a DFAS LAN, then DFAS must ensure that the LAN has the appropriate safeguards. Second, DFAS is responsible for establishing application controls for the financial application and for granting authorized access to the application. The DFAS must ensure that controls exist to prevent users from compromising the confidentiality, integrity, and availability of the data while users are in the financial application.

DISA Responsibilities. As the operator of the Defense megacenters, DISA has information assurance responsibility for the entry points from the various networks into the Defense megacenters. DISA is also responsible for each Defense megacenter internal network up to the point at which the user accesses the financial application. DISA responsibility extends to the controls over allowing access to the mainframe containing the financial application.

Performance of Risk Analysis

SOCOM, DFAS, and DISA are each responsible for information assurance. Therefore, to ensure confidentiality, integrity, and availability of SOCOM financial data, each organization must perform a risk analysis of the networks that they use to access the financial applications, as required by DoD Directive 5200.28.

Risk Analysis of SOCOM Networks. SOCOM has not conducted the required risk analysis of the unclassified networks that SOCOM personnel use to access financial applications that process SOCOM financial data. Further, SOCOM does not have any plans to conduct a risk analysis. SOCOM users access the financial applications using a variety of networks and access methods that SOCOM must review to ensure the confidentiality, integrity, and availability of the SOCOM financial data. Also, because most of the SOCOM organizations are tenants on military bases, SOCOM users often use the base metropolitan area network to access financial applications. To conduct a complete risk analysis of the network entry points, SOCOM must coordinate with the local base information systems security officer and obtain memorandums of agreement with the designated approval authorities for any networks connected to SOCOM networks as required by DoD Directive 5200.28. The memorandums of agreement should specify the security requirements for each organization.

Risk Analysis of DFAS Networks. The Inspector General, DoD, has an ongoing audit of the DFAS Enterprise LAN, a single standardized network for all DFAS locations to access the DFAS financial applications residing at the Defense megacenters. Therefore, this report makes no recommendation to analyze the risk of the DFAS networks.

Risk Analysis of Defense Megacenters. DISA initiated a certification and accreditation process for the operations at the Defense megacenters. Part of that process includes identifying all methods of access to the Defense megacenters and evaluating the vulnerabilities and risks associated with being connected to other networks. Therefore, DISA is fulfilling the requirement to perform a risk analysis.

Conclusion

Protecting the confidentiality, integrity, and availability of SOCOM financial data is the collective responsibility of SOCOM, DFAS, and DISA. The SOCOM, the owner of the data, must ensure that an unauthorized user cannot access the Defense megacenter and financial application through a SOCOM entry point. DFAS, as the owner of the financial application, is responsible for protecting all its network entry points and for implementing controls for the financial applications. DISA, as the owner of the computer system and the custodian of the financial data and application, is responsible for protecting the entry points to the computer system where the application resides and for protecting access to the financial application. DISA and DFAS have acted to carry out their respective responsibilities; however, SOCOM has yet to perform a risk analysis of its networks and entry points to other networks. Unless SOCOM identifies and implements appropriate security measures on its network and entry points to other networks used to access the financial systems, SOCOM cannot be assured that its financial data are adequately protected.

Recommendations and Management Comments

We recommend that the Commander in Chief, U.S. Special Operations Command:

1. Conduct a risk analysis for U.S. Special Operations Command unclassified networks and entry points to other networks that are used to access financial applications as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988.

Management Comments. The U.S. Special Operations Command concurred and plans to complete the risk assessments by July 1998.

2. Direct U.S. Special Operations Command organizations that are interconnected to other networks to enter into a memorandum of agreement with the applicable designated approval authority to specify the security

responsibilities associated with the interconnection of the networks, in accordance with DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988.

Management Comments. The U.S. Special Operations Command concurred and plans to complete all actions by July 1998.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

We reviewed overall information assurance and computer security for the financial applications and networks used to process and transmit SOCOM financial data used to support the DoD consolidated financial statements. Specifically, we:

- determined the Department 97 funds that SOCOM received for FY 1996;
- identified the sites that received SOCOM Department 97 funds or had manual or electronic input into the financial applications in FYs 1996 and 1997;
- identified the financial applications used to process SOCOM financial data;
- identified the communications systems and networks used to transmit SOCOM financial data;
- reviewed SOCOM, DFAS, and DISA security policies and procedures; and
- identified plans to protect the financial applications and data against compromise.

In addition, we interviewed accounting and finance personnel, security personnel, and computer and communications specialists at SOCOM, DFAS, and DISA locations.

Scope Limitation. We limited our review to the information assurance over the unclassified information systems and networks to process SOCOM unclassified financial data. While we reviewed SOCOM security policies and procedures, we did not conduct tests of the security systems.

Use of Computer-Processed Data. We did not use computer-processed data to determine the adequacy of the information assurance over the financial applications used to process SOCOM financial data.

Audit Period, Standards, Locations, and Contacts

We performed this financial related audit from June 1996 through April 1997. The audit was performed in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We visited or contacted individuals and organizations within the DoD. Further details are available on request.

Appendix B. Prior Audits and Other Reviews

General Accounting Office

Report No. AIMD-96-144 (OSD Case No. 1213), "DoD General Computer Controls: Critical Need to Greatly Strengthen Computer Security Program," August 1996. The report states that locations processing Navy and Marine Corps financial data have deficiencies involving security and access control, segregation of duties, physical and environmental protection, service interruption controls, and program change controls. Those deficiencies allow authorized and unauthorized users to improperly modify, steal, disclose, and destroy sensitive DoD data.

The report recommended that:

- the Secretary of Defense direct the DoD Chief Information Officer (CIO) to develop and implement a comprehensive DoD-wide computer security management program;

- the Secretary of Defense direct the Deputy Secretary of Defense to ensure that the duties established for the CIO for the Military Departments and Defense agencies include reporting on ongoing computer security efforts and activities to the DoD CIO for approval;

- the DISA Director and the CIO of the Military Departments and Defense agencies submit their policies and procedures to improve general computer controls to the DoD CIO for approval;

- the DoD CIO direct the DISA Director to develop and implement a comprehensive computer security program at the Defense megacenters;

- the CIO of the Military Departments and the Defense agencies submit to the DoD CIO for approval their plans to coordinate with DISA to improve computer controls affecting Defense megacenter operations; and

- the Secretary of Defense direct the DoD CIO to monitor and to periodically report on the status of the actions taken to implement the recommendations to improve computer security throughout the DoD.

Management generally concurred with the findings and recommendations. The DoD has completed corrective actions for three of the seven recommendations, and the information assurance working groups are still working on other recommended corrective actions.

Report No. AIMD-96-84 (OSD Case No. 1150), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risk," May 1996. The report states that the exact number of attacks on information systems cannot be readily determined because only a small number of computer attacks are detected and reported. The attacks are costly and pose a serious threat to national security. While DoD is attempting to react to the reported attacks, it has no uniform policy for assessing risk, protecting the systems, or reporting the incidents and assessing the damage. The report recommended that the Secretary of Defense strengthen the DoD information systems security program by:

- developing DoD-wide policies for preventing, detecting, and responding to attacks on DoD information systems;

- requiring the use of training and other mechanisms to increase awareness and accountability among personnel as to the security risks of systems connected to the Internet and designating responsibilities for securing the systems;

- requiring each installation to have an information systems security officer and setting standards for ensuring that the security officer is trained to perform assigned duties;

- continually developing and using department-wide network monitoring and protection technologies; and

- evaluating the incident response capabilities to ensure that they are sufficient to handle the projected threat.

The report also recommended that the Secretary of Defense assign clear responsibility and accountability within the Office of the Secretary of Defense, the Military Departments, and Defense agencies to ensure the successful

implementation of the security policies. Defense officials agreed with the report findings, conclusions, and recommendations and are taking corrective actions.

Office of the Inspector General, DoD

Report No. 96-124, "Selected General Controls Over the Defense Business Management System," May 21, 1996. The report states that the DFAS Financial Systems Activity, Columbus, Ohio, did not adequately protect the Defense Business Management System development code from compromise and did not adequately control program software changes. Also, the Defense Megacenter, Columbus, Ohio, and the Defense Logistics Agency System Design Center, Columbus, Ohio, were not adequately prepared to react to a disaster. Those weaknesses compromise the reliability of the financial statements and increase the risk of fraud, sabotage, and disruption of operations.

The report recommended that the DFAS Financial Systems Activity, Columbus, Ohio:

- strengthen access controls to properly secure the development system for the Defense Business Management System;
- improve the authorization process for software changes; and
- review selected portions of the existing software code based on risk of compromise.

The report also recommended that the Defense Megacenter, Columbus, Ohio, and the Defense Logistics Agency Systems Design Center, Columbus, Ohio, develop, finalize, and test a disaster recovery plan.

The DFAS has completed corrective actions for all recommendations. The DISA concurred with the recommendation to develop, finalize, and test the disaster recovery plan. The DISA developed and tested the disaster recovery plan. The Defense Logistics Agency concurred with the recommendation, except to periodically test its disaster plan. The Defense Logistics Agency is developing a disaster plan and will incorporate testing into the plan.

Report No. 95-259, "Internal Controls for the Military Sealift Command Portion of the Transportation Business Area of the FY 1994 Defense Business Operations Fund Financial Statements," June 28, 1995. The report states that general controls for accessing and accountability over the Unit Level Billing System were not effective and made the systems and data vulnerable to unauthorized access and alteration. The computer security personnel did not follow policies and procedures regarding access to the system and accountability of user identification codes. Also, security personnel were not adequately trained and supervised. The report recommended that the Commander, Military Sealift Command, do the following.

- Establish computer security policies that direct verification of the need for access and level of access and deletion of files and programs linked to user accounts after user identification codes are removed.

- Review periodically the user identification numbers and access levels as required by DoD Directive 5200.28, "Security Requirements for Automated Information Systems," April 1, 1985.

- Cancel user identification numbers upon termination of employment.

- Develop access procedures to restrict contractor employees to authorized tasks.

- Activate the Access Control Facility Version 2 software or other access software to establish an audit trail for detecting unauthorized access.

- Direct the automated data processing security officer to conduct periodic review of security operations for compliance with security procedures.

- Revise the security and training program for automated data processing systems security officers to provide more technical information on the Access Control Facility Version 2 software and to comply with the automated data processing training curriculum.

- Direct the automated data processing security officer to properly supervise computer security staff.

Management concurred with all the recommendations, and all the corrective actions have been completed.

Other Related Coverage

"Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," November 1996. The report states that information infrastructures are vulnerable to attack and that the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. No common vocabulary exists, and resources are focused on the classified content and systems. The DoD must preserve its ability to fulfill its basic mission and, therefore, must be concerned with maintaining the ability to perform critical functions and availability of the information necessary to fulfill those functions. Designing and protecting the infrastructure to avoid all risks is not feasible; however, the risk can be managed by protecting the critical portions. Monitoring, detection, damage control, and restoration must be performed at all levels.

The task force made the following 13 recommendations.

- Designate an accountable information warfare focal point.
- Organize for information warfare-defense.
- Increase awareness.
- Assess infrastructure dependencies and vulnerabilities.
- Define threat conditions and responses.
- Assess information warfare-defense readiness.
- Increase defenses with high-payoff, low-cost items.
- Establish and maintain minimum essential information infrastructure.
- Focus the research and development.
- Staff for success.
- Resolve the legal issues.
- Participate fully in critical infrastructure protection.
- Provide the resources.

Appendix C. List of Defense Finance and Accounting Service Locations

Centers

- Cleveland Center
- Denver Center
- Indianapolis Center
- Columbus Center
- Kansas City Center

Operating Locations

- Dayton, Ohio
- Omaha, Nebraska
- San Antonio, Texas
- Limestone, Maine
- San Bernardino, California
- Lexington, Kentucky
- Orlando, Florida
- Lawton, Oklahoma
- Rock Island, Illinois
- Seaside, California
- St. Louis, Missouri
- Rome, New York
- Charleston, South Carolina
- Norfolk, Virginia
- Oakland, California
- San Diego, California
- Honolulu, Hawaii

Operating Locations (cont'd)

- Pensacola, Florida
- Newark, Ohio
- Memphis, Tennessee
- Rantoul, Illinois

Appendix D. Financial Applications Used to Process U.S. Special Operations Command Financial Data

We identified the listed financial applications during the audit. The list may not include all financial applications that process SOCOM financial data.

Applications Used by SOCOM Army Components

- Standard Army Financial Systems
- Database Commitment Accounting System
- Standard Army Financial Inventory Accounting and Reporting System
- Program Budget and Accounting System
- Defense Civilian Payroll System
- Contract Accounts Payable System
- Integrated Automated Travel System
- Standard Army Financial System Redesign One

Applications Used by SOCOM Navy Components

- Standard Accounting and Reporting System
- Fleet Resource Accounting Module
- Program Budget and Accounting System
- Navy Headquarters Financial System
- Centralized Expenditure/Reimbursement Processing System

Applications Used by SOCOM Air Force Components

- Program Budget and Accounting System
- General Accounting and Finance System
- Integrated Accounts Payable System
- Security Assist Management Information System
- Central Procurement Accounting System
- Integrated Paying and Collecting System
- Standard Material Accounting System
- Job Order Cost Accounting System
- Finance Inventory Accounting and Billing System

Appendix E. Defense Megacenter Locations

- St. Louis, Missouri
- San Antonio, Texas
- Oklahoma City, Oklahoma
- Mechanicsburg, Pennsylvania
- Chambersburg, Pennsylvania
- Huntsville, Alabama
- Rock Island, Illinois
- Denver, Colorado
- Columbus, Ohio
- Dayton, Ohio
- San Diego, California
- Sacramento, California
- Warner Robins, Georgia
- Ogden, Utah
- Jacksonville, Florida
- Montgomery, Alabama

Appendix F. 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 (Command, Control, Communications, and Intelligence)

Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

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

Unified Commands

Commander in Chief, U.S. Special Operations Command
- Commander in Chief, Army Special Operations Command
- Commander in Chief, Naval Special Warfare Command
- Commander in Chief, Air Force Special Operations Command

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

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

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 Committee on Governmental Affairs
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

Part III - Management Comments

U. S. Special Operations Command Comments

UNITED STATES SPECIAL OPERATIONS COMMAND
OFFICE OF THE COMMANDER IN CHIEF
7701 TAMPA POINT BLVD.
MACDILL AIR FORCE BASE, FLORIDA 33621-5323

30 JUL 1997

MEMORANDUM FOR: DIRECTOR, READINESS AND OPERATIONAL SUPPORT, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Audit Report on Security Over Networks Used to Process U.S. Special Operations Command Financial Data (Project No. 6RE-2031)

1. Our management comments of the subject draft audit are attached. The audit discloses that risk assessments have not been conducted on USSOCOM unclassified systems used to access financial applications. The audit also recommends USSOCOM organizations which are interconnected to other networks enter into a memorandum of agreement with the applicable designated approval authority to specify security responsibilities associated with the interconnection of the networks.

2. USSOCOM concurs with the report findings and will implement actions based on the recommendations contained in the draft audit report. Information system security weaknesses have been noted throughout the Department of Defense .

3. USSOCOM appreciates the chance to provide management comments to the draft audit report. Our point of contact is Captain De La Garza, Computer Security Branch, DSN 968-4225.

Encl
as

HENRY H. SHELTON
General, U.S. Army
Commander in Chief

Audit Report on Security Over Networks Used to Process U.S. Special Operations Command Financial Data (Project No. 6RE-2031)

RECOMMENDATION 1: Conduct a risk analysis for U.S. Special Operations Command unclassified networks and entry points to other networks that are used to access financial applications as required by DOD Directive 5000.28, Security Requirements for Automated Information Systems," March 21, 1988.

USSOCOM COMMENTS: Concur. USSOCOM will begin conducting risk assessments of our unclassified systems which access financial data. The draft audit report identified 102 organizations that USSOCOM needs to conduct risk assessments on. USSOCOM plans to begin conducting risk assessments in July 1997 and complete them by July 1998. Also, during that period a new unclassified system is planned and a risk assessment will need to be conducted on that system.

RECOMMENDATION 2: Direct U. S. Special Operations Command organizations that are interconnected by other networks to enter into a memorandum of agreement (MOA) with the applicable designated approval authority to specify the security responsibilities associated with the interconnection of the networks, in accordance with DOD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988.

USSOCOM COMMENTS: Concur. USSOCOM will direct Command organizations that are interconnected to other networks to enter into a MOA with the applicable designated approval authority to specify security responsibilities. As risk assessments are conducted the designated approval authority will be determined and a MOA will be initiated. We plan to complete this recommendation as the risk assessments are completed. Completion date for this recommendation is July 1998.

Audit Team Members

This report was prepared by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Thomas F. Gimble
Salvatore D. Guli
Mary Lu Ugone
Cecelia A. Miggins
JoAnn Henderson
Scott S. Brittingham
Kimberly A. Slater
Nancy C. Cipolla