DEPARTMENT OF DEFENSE

AUDIT REPORT

DOD-WIDE AUDIT OF THE SECURE TERMINAL UNIT-III PROGRAM

No. 90-049

March 20, 1990

Office of the Inspector General

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

March 20, 1990

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)

SUBJECT: DoD-Wide Audit Report on the Secure Terminal Unit-III Program (Report No. 90-049)

This DoD-Wide summary report on the Audit of the Secure Terminal Unit (STU)-III Program is provided for your information and use. The STU-III is an unclassified, Government-approved telephone that can secure communications on commercial, Automatic Voice Network, or foreign telephone networks. As of July 1988, approximately 80,000 STU-III telephones had been ordered at a cost of about $272 million. The audit was made by the Office of the Assistant Inspector General for Auditing, DoD, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency from January 1988 through June 1989.

The objectives of the audit were to determine if requirements for STU-III's were consistently developed, adequately supported, and appropriately categorized and prioritized, and if the STU-III Program complied with DoD system acquisition procedures. The audit included an analysis of the funds budgeted and programmed from FY 1985 to FY 1991 to satisfy STU-III requirements and an evaluation of the effectiveness of applicable internal controls.

The DoD-wide audit disclosed that the STU-III Program was not effectively managed and controlled. Requirements were not consistently developed, adequately supported, or appropriately categorized and prioritized; contractor requirements were not identified; and adequate funds were not budgeted or programmed. As a result, there was no assurance that classified and the most sensitive information related to national security was being protected, or that DoD's investment in the STU-III Program was effectively used. In addition, the STU-III Program did not comply with the procedures for system acquisitions contained in DoD Directives 5000.1 and 5000.2. Therefore, the Defense Acquisition Board was excluded from major decisions relating to threat, affordability, acquisition strategy, alternative concepts, logistical support, and life-cycle costs.

We recommended that the Under Secretary of Defense for Policy revise DoD Regulation 5200.1-R to include guidance on protecting sensitive information during electronic transmission. We recommended that the Assistant Secretary of

Defense (Command, Control, Communications and Intelligence) revise DoD Directive C-5200.5 to include the responsibilities assigned under the 1985 realignment of the Office of the Secretary of Defense; establish guidance for identifying, categorizing, and prioritizing STU-III requirements; require DoD Components to recompute their requirements; review revised requirements for compliance with DoD policy; inform the Defense Acquisition Executive if total estimated production costs exceed the $1 billion threshold established in DoD Directive 5000.1; coordinate the requirements for additional STU-III's with the Comptroller of the Department of Defense and the Assistant Secretary of Defense (Program Analysis and Evaluation); formulate budget estimates; and recommend resource allocations in accordance with DoD Directive C-5200.5 (page 7).

A draft of this report was provided to the Under Secretary of Defense for Policy and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on October 16, 1989, for review and comments. Comments on the draft were received from the Under Secretary of Defense for Policy on January 9, 1990, and from the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on January 5, 1990.

The Under Secretary of Defense for Policy nonconcurred in Recommendation 1., which addressed revising DoD Information Security Program Regulation 5200.1-R, to include guidance for the protection of sensitive information during electronic transmissions. The Under Secretary stated that acceptance of the Recommendation would fundamentally alter the character of DoD Regulation 5200.1-R, and indicated that it would be more appropriate to incorporate the guidance by developing a new or modifying an existing DoD issuance. Establishing the guidance in new or existing regulations would satisfy the intent of our Recommendation. However, management comments did not indicate whether the corrective action would be taken or provide an estimated completion date.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred in Recommendation 2.a. through 2.f. The Assistant Secretary nonconcurred in Recommendation 2.g. of the draft report concerning reporting the lack of control over the implementation of the DoD-wide STU-III Program as a material internal control weakness. Management did not consider the reported deficiencies to be material. On the basis of the Assistant Secretary's comments, we deleted Recommendation 2.g. from the final audit report.

DoD Directive 7650.3 requires that all audit recommendations be resolved within 6 months of the date of the final report. Accordingly, the Under Secretary of Defense for Policy should provide final comments on the management action to be taken in response to Recommendation 1. within 60 days of the date of this memorandum.

The audit identified internal control weaknesses as defined by Public Law 97-255, Office of Management and Budget Circular A-123, and DoD Directive 5010.38. Controls were not established within the National Security Agency to identify initiatives that met the criteria established in DoD Directive 5000.1 for program management oversight by the Defense Acquisition Board. The recommendations, cited in the Office of the Assistant Inspector General for Auditing Report No. 89-069, "Secure Terminal Unit-III Program at the National Security Agency," if implemented, should establish adequate controls and eliminate the deficiency. DoD had not issued the appropriate guidance or provided sufficient oversight to effectively and efficiently direct, implement, and control the DoD-wide STU-III Program. Recommendation 2.a. through 2.f. in this report, if implemented, should correct these weaknesses. This report does not identify potential monetary benefits. The senior officials responsible for internal controls within the Office of the Secretary of Defense and the National Security Agency will be provided a copy of the final report.

The courtesies and cooperation extended to the audit staff are appreciated. If you have any questions concerning this audit, please contact Mr. Charles Santoni at (301) 859-6995 (AUTOVON 235-6311, extension 6995 FANX).

Susan J. Crawford

Susan J. Crawford
Inspector General

Enclosure

cc:
Under Secretary of Defense for Acquisition
Director, National Security Agency/Chief, Central Security Service
Director, Joint Staff

DOD-WIDE AUDIT OF THE
SECURE TERMINAL UNIT-III PROGRAM

TABLE OF CONTENTS

	Page
TRANSMITTAL MEMORANDUM/EXECUTIVE SUMMARY	i
PART I - INTRODUCTION	1
Background	1
Objectives and Scope	4
Prior Audit Coverage	5
PART II - RESULTS OF AUDIT AND RECOMMENDATIONS	7
APPENDIX A - Description of the Secure Terminal Unit-III	23
APPENDIX B - Audit Reports Issued on Secure Terminal Unit-III	25
APPENDIX C - Under Secretary of Defense for Policy Comments	27
APPENDIX D - Assistant Secretary of Defense (Command Control, Communications and Intelligence) Comments	29
APPENDIX E - Summary of Potential Monetary and Other Benefits Resulting from Audit	33
APPENDIX F - DoD-Wide Audit Team Members	35
APPENDIX G - Final Report Distribution	37

Prepared by:
Readiness and Operational
Support Directorate
Project No. 8IK-3001

DOD-WIDE AUDIT OF THE SECURE TERMINAL UNIT-III PROGRAM

PART I - INTRODUCTION

Background

The widespread use of telephone communications is essential to conduct the mission of the Department of Defense. However, all information transmitted on unsecured telephones is subject to hostile exploitation. Recognizing that information security is vital to the operational effectiveness of activities related to national security and military combat readiness, on September 17, 1984, the President signed National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security." NSDD 145 provides national objectives, policies, responsibilities, and an organizational structure to guide activities toward safeguarding systems that process or communicate classified or other sensitive information related to national security. Specifically, NSDD 145 provides that:

> systems that generate, store, process, transfer, or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation. . .systems that handle other sensitive, but unclassified, Government or Government-derived information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

DoD Directive (DoDD) C-5200.5, "Communications Security," October 6, 1981, states that measures shall be instituted within the Department of Defense to ensure that classified information is transmitted only by secure means and that unclassified information relating to the national security is protected during transmission. National Communications Security Instruction (NACSI) 6002, "Protection of Government Contractor Communications," June 4, 1984, requires protection of telecommunications between U.S. Government departments or agencies and their contractors as well as between U.S. Government contractors and their subcontractors. DoD Instruction (DoDI) 5210.74, "Security of Defense Contractor Telecommunications," June 26, 1985, establishes policy and procedures for securing and protecting telecommunications between and among DoD Components, their contractors, and subcontractors. The Instruction states that:

> first priority shall be given to providing a secure voice capability. . . and second priority. . .shall be given to securing record and data telecommunications among and between DoD program managers, and contractors and subcontractors who currently are performing on classified contracts and possess or routinely exchange significant amounts of classified information. Third priority shall be given to protecting unclassified national security related voice, record, and data telecommunications among program managers and their contractors and subcontractors.

NSDD 145, NACSI 6002, DoDD C-5200.5, and DoDI 5210.74 do not define sensitive, but unclassified information related to national security.

In 1983, the National Security Agency (NSA) initiated a study to determine if a low-cost secure telephone for widespread secure voice protection could be developed. Once the Agency determined that the concept was possible, it established a program office to develop and procure the Secure Terminal Unit (STU)-III telephone. NSA managed the STU-III Program as a Quick Reaction Capability (QRC) project, with a limited management plan and without a provision for Defense Acquisition Board oversight. The program office successfully developed the STU-III, which is considered a quantum leap in secure telecommunications. The STU-III is about twice the size of a standard telephone, relatively easy to use, and low in cost when compared to the cost of previous secure telephones. Appendix A describes the STU-III.

NSA's acquisition strategy for developing Communications Security (COMSEC) equipment is to communicate with commercial firms that are developing new communications products and assist these firms in incorporating secure capabilities into their products. As products enter the marketplace, DoD users can then directly purchase products with inherent secure capabilities, approved by NSA. NSA believed there would be large commercial as well as Governmental demands for secure telecommunications and automated information system products.

Although the STU-III was developed as an NSA project, a basic tenet of the STU-III acquisition strategy was that there would be a commercial demand for secure telephones and that STU-III's would be sold commercially. Once marketable, the commercial demand for STU-III's would help drive prices lower. Hence, lower prices, through commercial marketing, would allow the Government to purchase more secure voice protection.

In a memorandum entitled, "Security of Defense Telephone Communications," September 16, 1985, the Secretary of Defense

stated that national policy and good judgment mandate that classified and sensitive telecommunications be protected. He also indicated that bold and positive measures must be taken to ensure that Defense telecommunications are afforded the requisite degree of security. To achieve the degree of security needed, the Secretary required DoD Components to ". . .identify their total requirements for secure telephones to protect all classified and sensitive communications, and program adequate funds to purchase the required STU-III units within the 1987 to 1991 Five Year Defense Plan." For the purpose of identifying secure telephone requirements, the Secretary stated that DoD information that ". . .relates to operations, plans, system acquisition, logistics support, and personnel shall be considered sensitive, and must be protected."

The Secretary's guidance was intended to initiate a major expansion of communications security. Also, in 1985, the Commission to Review DoD Security Policies and Practices (the Commission) issued its report and recommended improving DoD's secure voice capabilities. In its report, "Keeping the Nation's Secrets," November 19, 1985, the Commission informed the Secretary of Defense that there were serious shortages of secure voice equipment needed to support DoD and its cleared contractors. The Commission stated that these shortages have led to "talking around" classified information over unsecured communications channels that were vulnerable to hostile intelligence interception. The Commission noted that it was aware of the importance of protecting sensitive, but unclassified information, terming it a monumental "security" problem, but did not interpret its charter as requiring an analysis in that area. The Commission did recognize and support NSA's initiative to provide low-cost secure communications on a broad scale.

In November 1985, the Joint Staff requested each DoD Component to estimate its total requirements for STU-III's. The estimates were to be based on the guidance contained in the Secretary of Defense's memorandum of September 16, 1985. The Joint Staff summarized the Components' requirements and, in July 1986, forwarded the summaries to NSA, the program manager for the STU-III. The Director for Command, Control, and Communications Systems of the Joint Staff put a caveat on the summarized requirements, stating, "As the survey did not consider fiscal constraints, the STU-III procurement by the Services and Agencies to satisfy all estimated requirements may not be possible in the time frame directed by the Secretary of Defense." Requirements for approximately 975,000 STU-III's were submitted by the DoD Components. These requirements generally excluded the STU-III's needed to secure telecommunications with Defense contractors. At the time of our audit, the cost of a STU-III was about $2,300. At the original target price of $2,000 each, 975,000 STU-III's would have cost about $1.95 billion. Funds had not been programmed to satisfy the level of STU-III requirements identified.

Objectives and Scope

The objectives of the audit were to determine if requirements for STU-III's were consistently developed, adequately supported, and appropriately categorized and prioritized, and if the STU-III Program complied with DoD system acquisition procedures. The audit included an analysis of the funds budgeted and programmed to satisfy STU-III requirements and an evaluation of the effectiveness of applicable internal controls.

The Dod-wide audit was made jointly by the Office of the Assistant Inspector General for Auditing, DoD, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency. Audits of OSD offices, Defense agencies, and Defense activities were made by the audit staff of the Assistant Inspector General for Auditing, DoD. Audits within the Services were made by the respective Service audit organizations. Overall, the audit was made at the OSD level, 13 Defense agencies and activities, the offices of the Services' headquarters responsible for the STU-III Program, and 50 major commands and field activities. The activities visited or contacted are listed in the reports listed at Appendix B that were used to compile this summary report.

The DoD-wide audit was made from January 1988 through June 1989. The audit was made in accordance with auditing standards for program results audits issued by the Comptroller General of the United States as implemented by the Inspector General, DoD, and accordingly included such tests of internal controls as were considered necessary.

The U.S. Army Audit Agency performed the audit from January through May 1988 at the Office of the Director of Information Systems for Command, Control, Communications, and Computers, Headquarters, Department of the Army; the Office of the Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army; five major Army commands; and four subordinate installations and activities. The Naval Audit Service audit was conducted from July through October 1987. The Naval Audit Service reviewed the computations of STU-III requirements made by 15 major commands and the documentation provided by 20 subordinate field activities. The Air Force Audit Agency performed its audit in March 1988 at the Office of the Assistant Chief of Staff, Systems for Command, Control, Communications, and Computers, Headquarters, Department of the Air Force; four major command headquarters; one operating agency headquarters; and Headquarters, Engineering and Installation Division, Air Force Communications Command.

Prior Audit Coverage

The Assistant Inspector General for Auditing, DoD, has not made a prior audit of the STU-III Program. The General Accounting Office (GAO) issued a report, GAO/NSIAD-86-7 (OSD Case 6880), "Concerns Regarding the National Security Agency Secure Telephone Program," October 15, 1985, which addressed the issue of whether appropriate criteria were being developed to justify the number of STU-III telephones that Government agencies would purchase. Of particular concern was the criterion for determining requirements to protect ". . .unclassified, but sensitive national security related information." The GAO report indicated that within the DoD, a high degree of confusion existed regarding the definition of this category of information, and that excessive expenditures to protect unclassified information could result if "sensitive" was too broadly defined. The DoD response to the report stated that the National Telecommunications and Information Systems Security Committee (NTISSC) was responsible for defining sensitive information. Once defined by the NTISSC, the Department of Defense would apply that definition to guide internal requirements. At the time of our audit, the NTISSC still had not developed an acceptable definition of sensitive information. The results of the DoD-wide audit confirmed GAO's concern.

In its report, GAO expressed concern that direct contractor purchases of STU-III telephones on a cost-reimbursable basis might result in excessive costs to the Government. The DoD responded that the significant size of the commercial market for secure telephones would preclude direct purchasers from being penalized by higher acquisition costs. The additional cost to DoD for contactor overhead and administrative costs was not addressed, and a significant commercial market has not materialized.

PART II - RESULTS OF AUDIT AND RECOMMENDATIONS

Management and Control of the Secure Terminal Unit-III Program

The results of the DoD-wide audit disclosed that the STU-III Program was not effectively managed and controlled. STU-III requirements were not consistently developed, adequately supported, or appropriately categorized and prioritized; contractor requirements were not identified; and adequate funds were not budgeted and programmed. These conditions occurred because the Office of the Secretary of Defense had not issued the appropriate guidance to effectively implement the STU-III Program DoD-wide. As a result, there was no assurance that classified and the most sensitive, but unclassified information related to national security was being protected, or that DoD's investment in the STU-III Program was being effectively used. In addition, the STU-III Program did not comply with the system acquisition procedures contained in DoD Directive 5000.1, "Major and Non-Major Defense Acquisition Programs," and DoD Instruction 5000.2, "Defense Acquisition Program Procedures." This condition occurred because the National Security Agency had not established internal procedures to identify and report initiatives that met major system acquisition criteria described in DoD Directive 5000.1. As a result, the Defense Acquisition Board was excluded from major decisions relating to threat, affordability, acquisition strategy, alternative concepts, logistical support, and life-cycle costs.

DISCUSSION OF DETAILS

Requirements Computation and Documentation. The DoD Components had various interpretations of the Secretary's memorandum on securing classified and sensitive telecommunications. As a result, a variety of methods were used to determine the quantity of STU-III's required. Considering most DoD-related information to be sensitive, most Components interpreted the Secretary's memorandum as a mandate to secure as many telephones as possible. Methodologies used to determine requirements included the number of telephones, the number of personnel, the availability of funds, comparisons with other DoD Components' requirements, and ratios. None of the methodologies distinguished between classified and sensitive, but unclassified requirements.

The DoD Components estimated their requirements for STU-III's in response to a 1985 tasking by the Joint Staff. The Joint Staff tasking letter used the definition of sensitive information that was included in the Secretary of Defense memorandum dated September 16, 1985. The DoD Components submitted requirements for approximately 975,000 STU-III's, exclusive of requirements for Defense contractors. Although the Secretary of Defense's memorandum stated that DoD telecommunications were to be afforded the "requisite degree of

security," DoD guidance was not issued to establish the criteria that the DoD Components were to use to determine the "requisite degree of security" or to validate their requirements. As a result, there was no assurance that the requirements established for protecting unclassified information were necessary or proportionate to the threat of exploitation and the associated damage to national security.

Army. The Army Audit Agency reported that the Army's STU-III requirements were not consistently developed nor adequately supported. Instead of basing requirements on actual needs, the Department of the Army submitted requirements to the Joint Staff based on a verbal agreement among the Services that each Service would report requirements for 300,000 STU-III's. Subsequently, all major Army commands and activities were requested to estimate their STU-III requirements. Even though the Commands' estimates showed unvalidated requirements for 516,000 STU-III's, the Army decided to maintain its original requirement at 300,000 units. The Army Audit Agency found that the estimated requirements computed by the major commands were not consistently developed, supported by adequate analyses, or validated. An evaluation of the requirements identified by 5 major commands (allocated about 53 percent of the Army's 300,000 requirements) showed significant differences in the procedures used to compute STU-III requirements. Although two major commands reported that they had significantly reduced their original requirements, their allocated portion of the overall Army requirement was not revised. Therefore, the Army's reported requirement for 300,000 units and the computed requirement for 516,000 units have not been validated, and both may be substantially overstated.

Department of the Army (DA) guidance for computing requirements did not define the types of sensitive, but unclassified information that should be protected and did not provide specific guidance for computing requirements. The Army Audit Agency concluded that because Army managers did not issue specific guidance, "the broad nature of DA guidance increased the subjectivity in determining requirements and allowed the major commands too much flexibility." The Army Audit Agency recommended that the Army develop specific guidance on the types of sensitive information to be protected and recompute requirements based on the specific guidance. The Army Audit Agency also recommended that approving officials review all revised computations along with supporting documentation for consistency and accuracy before approving the requirements. The Army agreed with the recommendations and stated that corrective action had been or would be taken.

Navy. The Naval Audit Service reported that the Navy had not provided sufficient guidance for computing STU-III requirements. As a result, the methods used to compute STU-III

requirements were not consistent, and STU-III requirements were inaccurate and generally not supportable. The Navy had originally reported a requirement of 300,000 STU-III's to the Joint Staff. At the time of the audit, the Navy had established an overall requirement of 277,900 STU-III's. The Naval Audit Service found that some commands had computed requirements based on replacing all of their telephones with STU-III's. Other commands planned to replace only a percentage of their existing telephones and used arbitrary percentages of authorized personnel billets to determine their requirement. In some cases, there was no documentation to support the requirements, or, where documentation was available, the requirements had been arbitrarily inflated. For example, the Naval Sea Systems Command (NAVSEA) had misplaced the documentation to support its requirement for about 74,290 STU-III's (about 27 percent of total Navy requirements). The Naval Audit Service reviewed requirements at six NAVSEA subordinate commands and found that four had submitted requirements that were subsequently inflated by NAVSEA. One subordinate command, the Naval Shipyard, Portsmouth, Virginia, submitted a requirement for 660 STU-III's. NAVSEA increased this requirement to 6,000 units. Similarly, the Naval Air Systems Command arbitrarily increased requirements computed by field activities from approximately 5,100 to 8,711 STU-III's.

The Naval Audit Service's review, although not statistically projectable, specifically identified requirements for 33,000 STU-III's that were based on unsupported or inflated data. These 33,000 units represented $79.7 million (about 12 percent) of the $666 million that the Navy estimated it needed to satisfy its STU-III requirements.

The Naval Audit Service recommended that the Navy develop comprehensive assessment and evaluation criteria to be used by commands for determining what specific sensitive, but unclassified information related to national security should be protected. The Naval Audit Service also recommended that the Navy require all commands to recompute their STU-III requirements to conform with the Navy's newly developed criteria and that the commands' requirements be validated for consistency and accuracy. The Navy concurred in the recommendations and indicated that a second requirements survey would be conducted using the definition of "sensitive" in the memorandum of the Secretary of Defense, September 16, 1985, and that the results would be monitored to ensure that inconsistencies are resolved.

Air Force. The Air Force Audit Agency reported that Air Force requirements were consistently developed, but were not adequately supported in accordance with Air Force regulations. The Air Force had originally estimated its STU-III requirements to be 300,000 units. In July 1987, the Assistant Chief of Staff, Systems for Command, Control, Communications, and Computers,

issued guidance for revalidating STU-III requirements to ensure that requirements were "reasonable" and consistent throughout the Air Force. The Air Force guidance specified that personnel who had a continuing requirement to discuss classified or sensitive information should have ready access to a secure telephone. The policy defined ready access as a sufficient number of STU-III's placed in a work area convenient to multiple users to support operational requirements. As a general rule, the Air Force defined "reasonable" as 15 users (plus or minus 10) per STU-III, depending on the operation. This definition resulted in a reduction of STU-III requirements to 57,000 units.

The Air Force Audit Agency reported that STU-III requirements for three of the four major commands and the one operating agency headquarters it reviewed had not been processed by the program management office of the Air Force Communications Command (AFCC) in accordance with Air Force regulations. Specifically, the program management office planned to procure STU-III's without ensuring that a validated communications-computer systems requirements document (CSRD) had been prepared. The program office accepted data directly from the major commands and operating agency headquarters via data disks without verifying that the requirements were properly supported by a validated CSRD. The program management office had not complied with applicable internal control procedures requiring that only validated communications-computer systems will be acquired. As a result, the Air Force acquired or planned to acquire STU-III's for unvalidated requirements. The Air Force Audit Agency recommended that the AFCC direct the program management office to process only validated STU-III requirements supported by a CSRD in compliance with Air Force regulations. The Air Force concurred in the recommendation and stated that the program office has advised the commands that validated CSRD's are required to justify the information on the data disks.

Defense Agencies. The Office of the Assistant Inspector General for Auditing reviewed the STU-III requirements for 13 Defense agencies and activities (Agencies). One Agency, the Washington Headquarters Services, was still in the process of determining and validating its requirements at the time of the audit. Of the remaining 12 Agencies, 10 were generally consistent in internally identifying and documenting their STU-III requirements. However, all 12 Agencies had different interpretations of the Secretary's memorandum and used various methodologies to develop their requirements. The overall result was that the Agencies were not consistent in computing requirements. Some Agencies had a liberal interpretation of the Secretary's guidance and planned to replace all telephones with STU-III's. Other Agencies took a more conservative approach and planned to replace only a portion of their telephones or none at all. The Office of the Assistant Inspector General for Auditing reported that the lack of specific DoD guidance on computing STU-III requirements represented an internal control weakness.

Contractor Requirements. DoD Instruction 5210.74, "Security of Defense Contractor Telecommunications," June 26, 1985, states that DoD policy is to secure or protect telecommunications among and between DoD Components, their contractors, and subcontractors in a manner that will preclude potential damage to the national defense. The Instruction includes provisions for the protection of classified and unclassified national security related voice, record, and data telecommunications among DoD program managers, and their contractors and subcontractors. Sensitive, but unclassified information related to national security is not defined in the Instruction. At the conclusion of the audit, the sole DoD guidance describing unclassified information to be protected was the Secretary of Defense's memorandum of September 16, 1985. Under this guidance, all Defense contractor and subcontractor telecommunications would need to be secured, regardless of the sensitivity of the information, the potential to adversely affect the national security, or cost. In addition, a pending change to the Federal Acquisition Regulation will establish a contract clause that will allow Defense contractors to secure their telecommunications with STU-III's and obtain reimbursement. However, the Services and Agencies did not generally identify contractor requirements for protecting classified and sensitive, but unclassified information related to national security other than replacing existing STU-II's with STU-III's.

Army. The Army Audit Agency found that its major commands and activities had not determined contractor requirements for STU-III's. Of the five major commands reviewed, only the Army Materiel Command had identified requirements for Defense contractors. The Materiel Command's estimated requirements were based on providing two STU-III's for each STU-II being used by its contractors. However, no major command determined whether its contractors had additional requirements to protect either classified or sensitive communications. Therefore, total contractor requirements for STU-III's were not determined.

The Army Audit Agency recommended that the Army establish detailed procedures for identifying contractor STU-III requirements. The Office of the Director of Information Systems, Headquarters, Department of the Army, agreed and stated that guidance would be issued to all commands to ensure that provisions for secure communications for contractors are considered as part of the overall contract.

Navy. The Naval Audit Service found that the Navy had identified few requirements for its contractors. A Chief of Naval Operations Note 2200, September 29, 1986, addressed DoD policy (DoD Instruction 5210.74) on securing contractor and subcontractor telecommunications. The Chief stated that requirements were being assessed, and further guidance would be

provided once requirements were determined and an acquisition method was selected. At the time of the audit, the method of acquisition had not yet been determined. The Naval Audit Service concluded that since the requirements generated by the Navy were in many cases linked to contractors, provisions should be made and an implementation plan should be developed to simultaneously coordinate Navy and contractor requirements.

The Naval Audit Service recommended that the Navy develop a plan for identifying and funding Defense contractor STU-III requirements in accordance with DoD Instruction 5210.74. The Navy concurred with the recommendation and stated that second-echelon commanders were requested to identify contractor requirements and establish an allocation plan to provide STU-III's as Government-furnished equipment.

Air Force. The Air Force Audit Agency concluded that all contractor requirements were not identified and included in the program funding process. The Office of the Assistant Chief of Staff, Systems for Command, Control, Communications, and Computers, and the AFCC program management office had not provided guidance to users to identify and fund STU-III's for Defense contractors. The Air Force Audit Agency concluded that because requirements may not be properly identified, STU-III's could be procured on a piecemeal basis, which could be more costly than consolidated procurements.

The Air Force Audit Agency recommended that the Assistant Chief of Staff, Systems for Command, Control, Communications, and Computers, direct the AFCC program management office to provide planning guidance to all major commands and operating agency headquarters to ensure that contractors' STU-III requirements are considered and, if appropriate, included in the validation process. The Assistant Chief of Staff concurred in principle and stated that the program management office informed the major commands and operating agency headquarters of the guidance in Air Force Regulation 700-10, "Information Systems Security." This Regulation gives program managers guidance on obtaining secure voice capabilities for contractors' communications.

Defense Agencies. Defense agencies planned to replace their contractors' STU-II's with STU-III's. However, the Agencies generally had not identified additional contractor requirements for STU-III's to protect classified telecommunications and sensitive, but unclassified information. Office of the Assistant Inspector General for Auditing Report No. 89-039, "Secure Terminal Unit-III Program at Defense Agencies and Activities," stated that the lack of specific DoD guidance regarding the identification of contractor requirements represented an internal control weakness. Office of the Assistant Inspector General for Auditing, Report No. 89-069, "Secure Terminal Unit-III Program at the National Security

Agency," recommended that the National Security Agency (NSA) determine its contractors' STU-III requirements and prioritize the distribution of STU-III's to be furnished to contractors. The NSA concurred and stated that it was attempting to insert a common language clause in each of its contracts that would permit the contractor to procure STU-III's and charge the cost to the Government.

Requirements Categorization and Prioritization. STU-III requirements were not prioritized to counter the most critical threats or to secure specific types of sensitive information. The majority of identified requirements were not categorized or prioritized by the classification, sensitivity, or type of information to be protected. Sensitive information is not included or defined in DoD Information Security Program Regulation 5200.1-R., or other DoD communications or information security directives, or instructions. DoD Directive C-5200.5, "Communications Security," had not been revised since 1981 even though a 1985 reorganization of the Office of the Secretary of Defense had transferred policy responsibility from the Under Secretary of Defense for Policy to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). Implementation of the STU-III Program was carried out under communications security policies issued before the initiation of the STU-III Program. Communications and information security policies were not revised to control the broad categories of information that the Secretary indicated were sensitive in his memorandum. No criteria were developed to ensure that unclassified information was assessed to determine its potential for damage to the national security if intercepted or that all classified and sensitive information requirements related to national security would be satisfied before satisfying requirements related to less sensitive information. Consequently, the STU-III Program may result in protecting unclassified information while classified or sensitive information related to national security remains unprotected. Additionally, the STU-III Program may fail to achieve its goal of an efficient and effective system of secure telecommunications within DoD.

Army. The Army Audit Agency found that STU-III requirements were not categorized by the type of information to be protected and ranked in order of priority. None of the five major commands reviewed had determined where the STU-III's would be located or had prioritized the distribution of the terminals. Only one of the five major commands reviewed had determined locations for distributing the STU-III's scheduled to be delivered in FY 1988. The major commands' requirements that had been prioritized represented only a small percentage of the STU-III's scheduled for distribution in FY 1988. For example, operating managers at the Army Training and Doctrine Command directed installations and activities to submit prioritized lists

of requirements for only the top 100, or 10 percent, of their requirements, whichever was less, and retain the remaining requirements for future submissions. Activities with few requirements submitted lists with as few as 2 STU-III's while activities with greater requirements submitted lists with as many as 100 STU-III's.

This procedure did not ensure that high priority requirements would be satisfied first. Some activities based requirements on replacing all standard telephones with STU-III's on a 1-for-1 basis; other activities limited their requirements to individuals having valid needs to discuss classified or sensitive information. Therefore, installations that only reported their high-priority requirements would initially receive only a few STU-III's. In another example, the Army Forces Command requested that its 24 subordinate activities develop and submit prioritized requirements for STU-III's scheduled to be delivered in FY 1988. Only 7 of the 24 activities submitted lists of their requirements. The Forces Command did not reattempt to obtain requirements from the remaining 17 activities. As a result, the Forces Command had no basis for satisfying the secure telephone requirements of users that had the most critical needs for protecting communications.

The Army Audit Agency recommended that the Army clarify responsibilities for implementing the Program; issue detailed guidance and procedures for prioritizing requirements; direct all activities and major commands to prioritize requirements based on the detailed guidance; and allocate STU-III's to major commands based on validated requirements. The Office of the Director of Information Systems, Headquarters, Department of the Army, agreed and stated that appropriate guidance would be provided to its field activities.

Navy. The Naval Audit Service found that the Navy had not adequately prioritized its STU-III telephone requirements for funding. The Navy considered approximately 100,000 of its requirement for 277,900 STU-III's to be the "minimum essential" to satisfy high-priority requirements. However, the Navy included about 12,000 low-priority STU-III telephones in the 52,630 units it had programmed for procurement through FY 1991. The Naval Audit Service recommended that the Navy prioritize its validated STU-III requirements to ensure that the "minimum essential" or high-priority requirements were funded before low-priority requirements. The Navy agreed with the recommendation.

Air Force. The Air Force Audit Agency found that overall, the Air Force had taken action to ensure that STU-III requirements were appropriately categorized and prioritized.

Defense Agencies. The Office of the Assistant Inspector General for Auditing reported that the Defense agencies had not categorized their requirements for protecting classified and sensitive information and had only prioritized those STU-III requirements that would be satisfied in the immediate future. Further, the agencies gave little consideration to external factors, for example, the need to contact other STU-III's to make a secure call. The lack of specific DoD guidance regarding the categorization and prioritization of STU-III requirements represented an internal control weakness.

The Office of the Assistant Inspector General for Auditing also disclosed that the plans established by the Defense Logistics Agency (DLA) and the NSA for distributing their STU-III's were unrelated to the need to protect all classified and the most sensitive, but unclassified information related to national security. Therefore, implementation of their plans may not result in the most effective use of the STU-III's purchased. Recommendations were made to the DLA and the NSA to improve the implementation of their internal STU-III programs by categorizing the information that needed to be discussed on their telephone systems, identifying the users that required secure telephones to protect information, and prioritizing the distribution of STU-III's accordingly.

DLA stated that it did not consider it practical to identify and prioritize the types of information that, if compromised, could adversely affect the national security. Further, DLA stated that, in its opinion, any attempt to identify and prioritize the specific users that require secure telephones would be extremely unreliable and no more likely to protect information than its STU-III distribution plan. The NSA concurred in the recommendation and agreed to recompute, categorize, and prioritize its requirements.

Funding. Sufficient funds had not been programmed DoD-wide to satisfy all identified requirements for STU-III's by FY 1991. The STU-III Program was managed by NSA, but responsibility for providing funding was decentralized to the individual DoD Components. No valid life-cycle cost data was prepared, but at NSA's target cost of $2,000 per STU-III, DoD's original requirement for 975,000 STU-III's would cost about $1.95 billion. Other than the replacement of existing STU-II equipment, requirements and funding for Defense contractors was unknown. DoD Components generally programmed insufficient funds to purchase requirements because of funding constraints or higher priorities for internal programs. Although the Army, Navy, and Air Force had each reported requirements for 300,000 STU-III's, only a fraction of those requirements had been funded. The funding issue was complicated because a consistent basis for computing or prioritizing requirements, to include the

requirements of Defense contractors, had not been established. Therefore, the total funding needed to satisfy valid STU-III requirements was not known.

Army. The Army originally programmed about $233 million in procurement funds for about 78,000 STU-III's. Budget cuts reduced its FY 1989 program from $29.9 million to $22.7 million, and the Army proposed to eliminate all funds programmed in FY's 1990 through 1994. The Army Audit Agency recommended that the Army compute future STU-III funding needs for use in the August 1988 budget review and maintain visibility and control by continuing to centrally program funds. The Army Audit Agency also recommended that controls be established to prevent major commands from acquiring duplicate secure and unsecure telephones. The Army agreed with the recommendations.

Navy. The Naval Audit Service reported that the Navy had programmed funds to procure only 52,630 STU-III's by FY 1991.

Air Force. The Air Force had centrally programmed funds through FY 1990 for 57,000 STU-III's.

Defense Agencies. Of the 13 agencies reviewed, 9 had funded or programmed funds to purchase all their STU-III requirements by FY 1993, and 2 planned to fund all their STU-III requirements beyond FY 1993. Although the DLA had funded a portion of its requirements, it did not program any funds for future procurements. The Washington Headquarters Services was still in the process of identifying and validating requirements at the time of the audit.

System Acquisition Procedures. DoD Directive 5000.1, "Major and Non-Major Defense Acquisition Programs," establishes policies, practices, and procedures to govern the acquisition of major and nonmajor Defense programs. According to the Directive, the Secretary of Defense shall designate those systems that are to be managed as major systems in accordance with DoD Directive 5000.1. The decision to designate any system as major may be based on one of the following criteria: estimated costs in FY 1980 dollars exceeding $200 million for research or $1 billion in eventual total expenditures for procurement, urgency of need, development risk, joint funding, or significant congressional interest. If designated as a major acquisition, the system is placed under the oversight of the Defense Acquisition Board (the Board). The Board advises and assists the Secretary of Defense, who makes decisions regarding acquisitions of major systems.

DoD Instruction 5000.2, "Defense Acquisition Program Procedures," provides uniform procedures and specific requirements for major acquisition programs. The procedures are also to be used in the management of nonmajor Defense acquisition programs. DoD

Instruction 5000.2 requires that the proponent of a program that meets DoD Directive 5000.1 criteria be able to provide documentation and support in a Mission-Needs Statement to provide a sound basis for decisions. The Mission-Needs Statement for a new acquisition program is required to include a discussion of the overall affordability of the program based on estimates of total research, development, test and evaluation costs; procurement costs; unit cost; and life-cycle cost. Each acquisition program must also address the system's mission and associated threat, alternative concepts, technology involved, funding implications, constraints, and acquisition strategy. This information provides the basis for informed management decisions at the start of a new acquisition program. As the acquisition program evolves, additional information is required at specified decision points to allow DoD management the opportunity to reevaluate the status of the acquisition program.

The Office of the Assistant Inspector General for Auditing found that the NSA did not recognize that the STU-III Program met criteria established in DoD Directive 5000.1 to identify systems that require program management oversight by the Board. Although the NSA estimated that the eventual procurement cost of the STU-III would exceed the $1 billion threshold, NSA had not established internal procedures to identify initiatives that met major system acquisition criteria.

The STU-III Program was managed as an internal quick-reaction project under NSA procedures rather than as a DoD-wide major acquisition. Consequently, the STU-III Program did not comply with DoD system acquisition procedures. NSA did not prepare the information for the STU-III Program required under DoD system acquisition procedures, and the Board was precluded from its oversight role. Board oversight of the Program would have addressed at the OSD level the issues of threat, affordability, acquisition strategy, alternative concepts, and life-cycle cost. In addition, operational testing was delayed, and full-scale production decisions were made before test results were reported to Congress. Compliance with DoD system acquisition procedures would have addressed and resolved some of the issues surrounding the Program, such as the validity of requirements, scope of production, acquisition strategy, and funding status in the preliminary stages of the STU-III Program.

The Office of the Assistant Inspector General for Auditing recommended that NSA recognize the STU-III Program as a candidate for a DoD-wide major acquisition and submit a Mission-Needs Statement to the Defense Acquisition Board. Another recommendation provided that NSA include procedures and criteria for identifying programs subject to the provisions of DoD Directive 5000.1 in its internal regulations and report the lack of procedures to identify programs meeting DoD Directive 5000.1

criteria as a material weakness in its annual assurance statement to the Secretary of Defense. NSA agreed to revise its internal regulations, but disagreed with the remaining recommendations. NSA stated that it firmly believed that the STU-III was not a major system acquisition since funds budgeted and programmed in the Five Year Defense Plan for the STU-III Program did not exceed the $1 billion threshold established by the Directive. NSA's interpretation of the Directive is that a program does not meet major system acquisition thresholds unless the funds are actually budgeted and programmed in the Five Year Defense Plan. The Office of the Assistant Inspector General for Auditing contended that NSA's interpretation was not supported by the guidance contained in DoD Directive 5000.1. The Directive clearly states that a Mission-Needs Statement is required for all acquisitions with eventual total production costs in excess of $1 billion. Internal NSA estimates of production costs during development of the STU-III were in excess of the $1 billion threshold. The requirement figures reported to the NSA by the Joint Staff also indicated eventual total production costs would be well above the production thresholds established in DoD Directive 5000.1.

Pursuant to the provisions of DoD Directive 7650.3, the disputed recommendations were referred to the Office of the Assistant Inspector General for Analysis and Followup, DoD, for mediation. On November 7, 1989, the Assistant Inspector General for Auditing and the Comptroller, NSA, reached an agreement that resolved the disputed issues. Both parties agreed that there was uncertainty as to the validity of the STU-III requirements submitted by the DoD Components and that the DoD policy for computing STU-III requirements needed clarification. The Comptroller stated that NSA considered these factors, interpreted the requirements that were submitted, and made a conscious decision not to report the STU-III Program as a major acquisition system. The Comptroller agreed to comply with the reporting requirements of DoD Directives 5000.1 and 5000.2 if the STU-III requirements being recomputed in response to Recommendation 2.c. of this report meet the criteria for designation as a major system acquisition. Based on the issues involved, the Assistant Inspector General for Auditing agreed to drop the recommendation to report the absence of detailed procedures as a material weakness in the NSA's annual assurance statement to the Secretary of Defense. It was agreed that the absence of procedures was a control weakness at the agency level.

Internal Controls. DoD Directive 5010.38, "Internal Management Control Program," dated April 14, 1987, specifies procedures for identifying and reporting weaknesses in management controls. The Directive (Enclosure 4, Section B.1.) refers to weaknesses in terms of both lack of applicable internal controls and inadequate compliance with existing controls.

Adequate policies and plans had not been promulgated by Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) to efficiently and effectively implement and control a DoD-wide secure telecommunications system. DoD Directive C-5200.5, "Communications Security," and DoD Regulation 5200.1-R, "DoD Information Security Program Regulation," were not revised to provide clear direction to and control over a major expansion of the information security program. Further, sufficient guidance was not provided to DoD Components to enable them to consistently develop, adequately support, and appropriately categorize and prioritize their requirements for STU-III's. The lack of clarity in program direction was the primary cause of the conditions noted in the reports of the Service Audit Agencies and the Office of the Assistant Inspector General for Auditing, listed in Appendix B, that were used to compile this DoD-wide report.

DoD Directive 5000.1, "Major and Non-Major Defense Acquisition Programs," establishes criteria for identifying candidates for major system acquisition oversight. NSA did not recognize that the STU-III Program met these criteria. This weakness occurred because the NSA did not have a control mechanism to ensure that the OSD Directive was being followed.

Conclusion. The efforts of NSA and the DoD Components have improved the quality and quantity of communications security DoD-wide. However, to derive the optimum benefit from the STU-III Program, DoD Component and Defense contractor networking is required. Such networking would ensure that STU-III's are deployed throughout the DoD and DoD-related industry in a time frame and sequence adequate to provide communications security and to allow classified or sensitive discussions among and between the DoD Components and Defense contractors. DoD-wide policies are necessary to provide consistent guidance on information to be secured by all DoD Components and Defense contractors and to establish a logical priority sequence for implementation. The basic problem is that, even though acceptance of the need to secure telecommunications with STU-III's was rapid, all requirements have not been funded and may not be funded in the future. Implementation of the STU-III Program will have only limited effectiveness if the DoD Components and Defense contractors do not have access to STU-III's.

RECOMMENDATIONS FOR CORRECTIVE ACTION

1. We recommend that the Under Secretary of Defense for Policy revise DoD Information Security Program Regulation 5200.1-R to include guidance for the protection of sensitive information during electronic transmission.

2. We recommend that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence):

a. Revise DoD Directive C-5200.5 to document changes in organizational responsibilities under the 1985 realignment of the Office of the Secretary of Defense.

b. Establish guidance for the consistent computation of DoD Components and Defense contractor STU-III requirements to protect classified information, sensitive information related to national security, and other sensitive information. The guidance should include procedures for categorizing the information to be protected and for prioritizing requirements.

c. Require DoD Components to recompute their STU-III requirements based on the guidance established.

d. Review the total requirements and priorities submitted by DoD Components for compliance with DoD policy.

e. Inform the Defense Acquisition Executive of the Defense Acquisition Board if the estimated eventual total production cost for the recomputed STU-III requirements (on hand, funded, and unfunded) exceeds the $1 billion threshold established by DoD Directive 5000.1.

f. Coordinate resource requirements with the Comptroller of the Department of Defense and the Assistant Secretary of Defense (Program Analysis and Evaluation) for additional STU-III telephones to complete an acceptable STU-III capability; formulate budget estimates; and recommend resource allocations in accordance with DoD Directive C-5200.5, "Communications Security."

MANAGEMENT COMMENTS

The Under Secretary of Defense for Policy nonconcurred in Recommendation 1., and noted that DoD Regulation 5200.1-R has historically provided implementing guidance for safeguarding only classified information. Management stated that acceptance of the Recommendation would fundamentally alter the character of the Regulation and indicated that it would be more appropriate either to develop a new regulation or to modify an existing regulation.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred with Recommendation 2.a. through 2.f. and provided planned or actual completion dates for corrective actions.

AUDIT RESPONSE TO MANAGEMENT COMMENTS

The expansion of Communications Security doctrine to include sensitive, but unclassified telecommunications fundamentally

alters DoD's approach to information security. DoD policy requires that sensitive, but unclassified information be encrypted. The same or similar devices that encrypt classified information can be used to protect sensitive, but unclassified information. Therefore, the DoD information security program has been fundamentally altered, even if DoD 5200.1-R has not been changed. Although we believe that guidance pertaining to the protection of DoD information should be presented in the Information Security Program Regulation, incorporating the guidance in another regulation or a new regulation would satisfy the intent of the Recommendation.

DESCRIPTION OF THE SECURE TERMINAL UNIT-III

STU-III Telephone. The Secure Terminal Unit (STU)-III is an unclassified, Government-approved telephone that can secure all classified and unclassified information discussed on commercial, Automatic Voice Network, or foreign telephone networks. Each unit is modular, transmits voice and data, and operates in the secure and clear modes.

Secure conversations are possible only when other STU-III telephones are called. For each secure call, the STU-III uses a traffic encryption key (TEK) to encrypt (encode) the information for the duration of the call. Each STU-III cooperates in establishing the TEK by generating a portion of it. Unlike the STU-II (Secure Terminal Unit-II), interaction with a separate key distribution center is not required for a secure call setup. A new TEK is established for each call. The STU-III's Key Encryption Keys (KEK) protect the exchange of the two portions of the TEK. KEK's may be obtained and placed in a STU-III either physically or electronically.

To reduce the physical security requirements on a STU-III terminal containing a KEK, each terminal is protected from unauthorized use by a Crypto Ignition Key (CIK). The CIK is a physical device that must be inserted in a STU-III to activate the secure mode. If the CIK is not inserted, the STU-III can be used as an ordinary telephone.

Once a STU-III call is secured, a display will show the identification of the distant telephone and the highest common level (unclassified, confidential, secret, or top secret) of information that can be discussed. In addition, the STU-III's can display whether both telephones are authorized for discussion of compartmented information, such as special intelligence. The STU-III telephones verify whether they have two-digit compartmentation codes in common, and if so, the STU-III's display the particular compartment.

Key Management System. The keying material used by the STU-III's is generated and distributed by the Key Management System (KMS). KMS functions are divided between the Key Management Center (KMC) and the Key Material Ordering and Distribution Center (the Center). Both activities are collocated at Finksburg, Maryland, and are under the operational control of the National Security Agency. The KMC prepares customized keys by combining user-specified identification information and Agency-generated cryptographic information. Orders for keys are checked against a data base of activities authorized to request keys. STU-III users must call the KMC once a year to have their STU-III's electronically rekeyed. The Center processes orders and ships keys to the requesting activity. The Center also maintains accountability records and monitors security compromises as they are reported.

AUDIT REPORTS ISSUED ON SECURE TERMINAL UNIT-III

Department of the Army

Army Audit Agency, Report No. HQ 89-600, "Requirements for the Secure Terminal Unit-III Program," December 2, 1988

Department of the Navy

Naval Audit Service, Report No. 7546/096-S-88, "Establishing Secure Terminal Unit-III Telephone Requirements," April 5, 1988

Department of Air Force

Air Force Audit Agency, Report No. 8215212, "DoD-Wide Review of Secure Telephone Unit-III Requirements," January 30, 1989

Other DoD Activities

Inspector General, Department of Defense, Audit Report No. 89-039, "Secure Terminal Unit-III Program at Defense Agencies and Activities," December 9, 1988 (Classified Report)

Inspector General, Department of Defense, Audit Report No. 89-045, "Secure Terminal Unit-III Program at the Defense Logistics Agency," 89-045, January 10, 1989

Inspector General, Department of Defense, Audit Report No. 89-069, "Secure Terminal Unit-III Program at the National Security Agency," April 20, 1989 (Classified Report)

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D C 20301-2000

POLICY

0 6 JAN 1990
In reply refer to:
I-89/60902

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Draft Summary Report on the DoD-Wide Audit of the Secure Terminal Unit-III Program (Project No. 8IK-3001.00)

This is in response to your 16 October 1989 memorandum whereby you provided a copy of the subject report for our comments on the finding addressed to the Under Secretary of Defense for Policy.

One of your recommendations was addressed to this organization, namely, "1. We recommend that the Under Secretary of Defense for Policy revise DoD Information Security Program Regulation 5200.1-R to include guidance for the protection of sensitive information during electronic transmission."

I do not concur with this recommendation. Since 1972, the Regulation has provided the DoD implementation of Executive orders governing the security classification and safeguarding of national security information, that is, that which is Confidential, Secret, or Top Secret. Acceptance of the recommendation would fundamentally alter the character of DoD 5200.1-R. I am, however, tasking the staff to study the feasibility of developing a new or modifying an existing DoD issuance other than DoD 5200.1-R that would address the protection issue raised by your recommendation. Related to this action, we will ask the Office of General Counsel to render an opinion on whether the Computer Security Act of 1987 is an Act within the scope of the third Freedom of Information Act exemption. If so, the Department's procedures for the protection of "For Official Use Only" information may apply.

Your report notes that the Department of Defense has yet to adopt a definition of sensitive but unclassified information. The Computer Security Act of 1987 provides a definition for purposes of processing such information in computer systems. The current draft of DoD Directive C-5200.5, "Communications Security (COMSEC)," uses the same definition. Accordingly, that definition will be our departure point.

Mr. David E. Whitman in my Security Plans and Programs Directorate has the action on this matter. He may be contacted on x52289 or x52686 in the event of questions.

Craig Alderman, Jr.
Deputy (Security Policy)

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

28 DEC 1989

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING

SUBJECT: Draft Summary Report on the DoD-Wide Audit of the Secure Terminal Unit-III Program (Project No. 8IK-3001.00)

This memorandum is in response to your request for comments on the subject draft audit report, dated 16 October 1989. The objectives of the audit were to determine if requirements for STU-III's were consistently developed, adequately supported, and appropriately categorized and prioritized, and if the STU-III Program complied with the DoD system acquisition procedures.

This office generally concurs with the draft report, and has initiated actions to implement recommendations 2.a through 2.f. Since revalidation actions and other initiatives recommended are underway, and since no evidence of fraud, waste or abuse has been cited in the audit report, we consider the noted control deficiencies as being non-material. Therefore, nonconcur in the retrospective reporting of the previous deficiencies as an internal management control problem.

Albert R. Lubarsky
Deputy Assistant Secretary of Defense
(Command, Control and Communications)

Attachment

DODIG DRAFT REPORT- DATED OCTOBER 16, 1989

PROJECT NUMBER 8IK-3001.00

DOD-WIDE AUDIT OF THE STU-III PROGRAM

ASD(C3I) COMMENTS

* * * * *

RECOMMENDATIONS

RECOMMENDATION 2.a: That the ASD(C3I) revise DoD Directive C-5200.5 to document changes in organizational responsibilities under the 1985 realignment of the Office of the Secretary of Defense.

ASD(C3I) POSITION: Concur. The revision to DoD C-5200.5 is currently being formally staffed with the DoD Components. Action officer meetings have been held to resolve substantive comments, and publication is expected within 60 days. The revised C-5200.5 will require that classified national security information be transmitted only by secure means, and that sensitive information be protected during transmission to the level of risk and magnitude of harm as determined by the cognizant DoD component head or representative. In addition, the new C-5200.5 will include a definition of sensitive information and a provision to ensure the security or protection of telecommunications between and among DoD components, contractors and subcontractors.

PLANNED ACTIONS: ASD(C3I) will complete C-5200.5 revision as recommended (March 1990).

RECOMMENDATION 2.b: That the ASD(C3I) establish guidance for the consistent computation of DoD and Defense contractor STU-III requirements to protect classified information, sensitive information related to national security, and other sensitive information. The guidance should include procedures for categorizing the information to be protected and for prioritizing requirements.

ASD(C3I) POSITION: Concur. Besides the general COMSEC guidance found in the C-5200.5 revision mentioned above, the ASD(C3I), in coordination with the Joint Staff and the DoD IG, sent a message to all DoD Components last April (241832Z APR 89), Subject, STU-III Family Requirement Revalidation. This message provided definitive guidance on the priorities and categories of information to be protected when determining STU-III requirements. In addition to listing the priorities and categories of information to be considered in determining STU-III requirements, this message also defined sensitive information. Briefly put, four fielding priorities and seven categories of information in descending order of importance were outlined in this message. This message also

contained guidance on the protection of communications between DoD and contractors (including subcontractors) that involve, for example, the technologies currently listed in the Military Critical Technologies List published by the Under Secretary of Defense for Research and Engineering.

PLANNED ACTIONS: Except for final publication of the aforementioned revision to DoD Directive C-5200.5, this action has been completed.

RECOMMENDATION 2.c: That the ASD(C3I) require DoD Components to recompute their STU-III requirements based on the guidance established.

ASD(C3I) POSITION: Concur. ASD(C3I) has tasked the Joint Staff to compile the STU-III requirements called for in the aforementioned April 24, 1989, message. The Joint Action associated with the revalidation effort is now in the final stages of coordination.

PLANNED ACTIONS: None beyond what is stated above. The Joint Action computations are being revalidated by all components as part of the coordination effort.

RECOMMENDATION 2.d: That the ASD(C3I) review the total requirements and priorities submitted by the DoD Components for compliance with DoD policy.

ASD(C3I) POSITION: Concur. A review of the total STU-III requirements and priorities submitted by the DoD Components will be accomplished, pending the completion of the aforementioned Joint Action.

PLANNED ACTIONS: None beyond what is stated above.

RECOMMENDATION 2.e: That the ASD(C3I) inform the Defense Acquisition Executive of the Defense Acquisition Board if the estimated eventual total production cost for the recomputed STU-III requirements (on hand, funded, and unfunded) exceeds the $1 billion threshold established by DoD Directive 5000.1.

ASD(C3I) POSITION: Concur. The total cost of the STU-III Program is expected to be approximately $750 million. The final draft version of the aforementioned Joint Action to revalidate total STU-III requirements indicates a total need of 313,247 STU-III's. It is therefore highly unlikely that the total cost of the program will exceed the $1 billion Defense Acquisition Board threshold.

PLANNED ACTIONS: None, unless the total estimated STU-III requirement is estimated to be more than 400,000 units.

RECOMMENDATION 2.f: That the ASD(C3I) coordinate resource requirements with the Comptroller of the Department of Defense

and the Assistant Secretary of Defense (Program Analysis and Evaluation) for additional STU-III telephones to complete an acceptable STU-III capability; formulate budget estimates; and recommend resource allocations in accordance with DoD Directive C-5200.5, "Communications Security."

ASD(C3I) POSITION: Concur. Once the STU-III requirements have been finalized, resource allocations to complete an acceptable STU-III capability will be coordinated as recommended. Currently, DoD Components have set aside funds for, or have already acquired over two-thirds of the estimated STU-III needs. An additional $220 million may be necessary to completely buy out the STU-III program, this resource estimate will have to compete with other high priority needs during the normal budgetary process.

PLANNED ACTIONS: Total resource requirements to complete the STU-III fielding is expected to be known by March 1990, and will be entered into the budgetary process as soon as they are finalized.

RECOMMENDATION 2.g: That the ASD(C3I) report the lack of control over the implementation of the DoD-Wide STU-III Program as a material weakness to the Secretary of Defense in the annual statement on the adequacy of internal management controls and track the material weakness as required by DoD Directive 5010.38, "Internal Management Control Program."

ASD(C3I) POSITION: Non-Concur. Although guidance to DoD Components for computing STU-III requirements may have been unclear when the STU-III program was initiated in 1985, recent revalidation actions, which were coordinated with the Joint Staff, the DoD IG, and the Components have resulted in adequate guidance for determining STU-III requirements. Since the report did not find any evidence of waste, fraud, loss, unauthorized use or misappropriation of government assets, and the report did not identify potential monetary benefits, the necessity to report a lack of control over the implementation of the STU-III Program as a material weakness in the annual report to the Secretary of Defense seems inappropriate. As stated in the report the implementation of recommendations 2.a through 2.f should correct the noted weaknesses.

SUMMARY OF POTENTIAL MONETARY AND OTHER BENEFITS RESULTING FROM AUDIT

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
1.	Program Results - Provides guidance for protecting sensitive information.	Nonmonetary
2a.	Internal Control - Specifies the changes in responsibilities resulting from the 1985 reorganization of the Office of the Secretary of Defense.	Nonmonetary
2b.	Program Results - Provides guidance for consistent computation of STU-III requirements to protect classified and sensitive information, including procedures for categorizing and prioritizing requirements.	Nonmonetary
2c.	Program Results - Establishes a realistic requirement that is consistent among the Services for planning secure telecommunications.	Nonmonetary
2d.	Internal Control - Provides reasonable assurance that DoD-wide requirements and priorities comply with DoD guidance and form a reasonable basis for planning secure telecommunications.	Nonmonetary
2e.	Internal Control - Alerts the Defense Acquisition Board if STU-III requirements exceed the threshold for major acquisition system oversight.	Nonmonetary
2f.	Economy and Efficiency - Provides the mechanism for funding to complete an acceptable STU-III capability.	Nonmonetary

DOD-WIDE AUDIT TEAM MEMBERS

Office of the Assistant Inspector General for Auditing

William F. Thomas, Director, Readiness and Operational Support
Charles M. Santoni, Program Director
Wade T. Najjum, Project Manager
H. Phillip Davis, Project Manager
Linda Freeman, Team Leader
John Betar, Team Leader
Larry J. Piatz, Team Leader
Stephen M. Dudiak, Auditor
Thomas Sidell, Auditor
Dale Katzenberger, Auditor

Army Audit Agency

James A. Nirschl, Assistant Director
Bruce Marsh, Auditor in Charge

Naval Audit Service

J. H. Stafford, Assistant Director
W.F. Hooper, Auditor in Charge

Air Force Audit Agency

Arthur Barker, Associate Director
James Simon, Audit Manager

FINAL REPORT DISTRIBUTION

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications and Intelligence
Assistant Secretary of Defense (Program Analysis and Evaluation)
Assistant Secretary of Defense (Public Affairs)
Comptroller of the Department of Defense
Assistant to the Secretary of Defense (Intelligence Oversight)
Assistant to the Secretary of Defense (Intelligence Policy)
Director, Joint Staff

Department of the Army

Secretary of the Army
Assistant Secretary of the Army (Financial Management)
Auditor General, U.S. Army Audit Agency
Army Inspector General

Department of the Navy

Secretary of the Navy
Assistant Secretary of the Navy (Financial Management)
Comptroller of the Navy
Auditor General, Naval Audit Service

Department of the Air Force

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

Defense Activities

Director, Defense Advanced Research Projects Agency
Director, Defense Communications Agency
Director, Defense Contract Audit Agency
Director, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, Defense Mapping Agency
Director, National Security Agency/Chief, Central Security Service
Director, Defense Nuclear Agency
Director, Defense Security Assistance Agency
Director, Defense Investigative Service
Director, Defense Logistics Studies Information Exchange

Non-DoD Activities

White House Communications Agency
Office of Policy Development, National Security Council
National Security Telecommunications Advisory Committee
Office of Management and Budget
General Accounting Office
  NSIAD Technical Information Center

Non-DoD Activities (Continued)

Congressional Committees:

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Ranking Minority Member, Committee on Armed Services
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Ranking Minority Member, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations
House Permanent Select Committee on Intelligence
House Subcommittee on Oversight and Evaluation, Permanent Select Committee on Intelligence