

~~FOR OFFICIAL USE ONLY~~

*A*udit



*R*eport

SPECIAL ACCESS PROGRAM SECURITY ISSUES

Report No. 98-089

March 11, 1998

Office of the Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~

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 or visit the Inspector General, DoD, home page at: WWW.DoDIG.OSD.MIL.

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) 604-8908 (DSN 664-8908) 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

DCII	Defense Clearance and Investigations Index
NISPOM	National Industrial Security Program Operating Manual
PAR	Program Access Request
SAP	Special Access Program

~~FOR OFFICIAL USE ONLY~~



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

March 11, 1998

MEMORANDUM FOR DEPUTY TO THE UNDER SECRETARY OF DEFENSE
FOR POLICY FOR POLICY SUPPORT
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, SPECIAL ACCESS PROGRAM
COORDINATION OFFICE
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Special Access Program Security Issues
(Report No. 98-089)

We are providing this report for review and comment. This report is the second of two audit reports on special access program security issues. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires prompt resolution of all recommendations. As a result of management comments, we revised draft Recommendation A.3. to the Chief, Technology Management Office, Army Staff, to incorporate his proposed alternative action. Because the Air Force did not specifically respond to Recommendation A.4. in the draft report, we ask that it comment on that recommendation in response to the final report by May 11, 1998.

We appreciate the courtesies extended to the audit staff. Please direct questions on the audit to (b)(6) Audit Program Director, at (703) 604-(b)(6) (DSN 664-(b)(6)) or (b)(6) Audit Project Manager, at (703) 604-(b)(6) (DSN 664-(b)(6)). See Appendix F for the report distribution. The audit team members are listed inside back cover.

A handwritten signature in black ink that reads "Robert J. Lieberman".

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-089

(Project No. 7AD-0005 01)

March 11, 1998

Special Access Program Security Issues

Executive Summary

Introduction. This report is the second of two audit reports on special access program security issues. A special access program is any program designed to control access, distribution, and protection of sensitive information. This report addresses the implementation of the National Industrial Security Program Operating Manual Supplement (the Supplement) and the use of standardized administrative documentation, program access requests, and protective markings within special access programs. Executive Order 12829, "National Industrial Security Program," January 1993, established the National Industrial Security Program as a single, integrated, cohesive industrial security program to protect classified information and to preserve information vital to the Nation's security. The Supplement, issued February 1995, provides mandatory and 45 optional enhancements for the protection of information used in special access programs and compartmented efforts similar to special access programs. The Department of Defense is the Federal Government Executive Agent of the Supplement. We conducted the audit at 22 special access program offices and 22 contractor facilities.

Audit Objective. The overall audit objective was to evaluate areas in which improvements in the efficiency and effectiveness of special access program security policies, procedures, and practices can be made. Specifically, we reviewed the DoD Components' implementation of the Supplement and the adequacy of special access administrative processes and forms. The audit also evaluated the adequacy of the management control program as it applied to the audit objectives. Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs," February 10, 1998, addresses our review of access reciprocity within DoD.

Audit Results. We identified issues relating to the implementation of the Supplement and administrative requirements.

- o The DoD special access community did not fully and effectively implement the Supplement. As a result, DoD Components provided their special access program contractors with redundant and conflicting security guidance. Consequently, contractors with multiple special access programs were unable to establish efficient, security-related business processes within their facilities (Finding A).

- o DoD special access programs subjected the contractors that deal with multiple special access programs to inefficient, redundant, and unclear administrative requirements. The inefficient and redundant requirements were burdensome and confusing to contractors, increased contractor overhead cost, and had the potential for delaying performance on special access program contracts (Finding B).

~~FOR OFFICIAL USE ONLY~~

Although our audit primarily focused on special access programs that the Military Departments managed, senior officials within the special access program community stated that the problems identified in the audit also applied to the Defense agencies.

Summary of Recommendations. We recommend issuing guidance to meet the intent of the Supplement as the single, integrated document that provides protective options for special access programs and developing policy to implement the Single Process Initiative within DoD special access programs. We also recommend that the Army issue guidance to Army special access programs that categorizes special access programs as waived, unacknowledged, or acknowledged so that the programs can interpret guidance from DoD. Finally, we recommend that the Air Force use the suggested menu of options that the Director, Special Access Program Coordination Office, established to standardize the Supplement's protective options within each special access program category (Finding A).

We recommend that the appropriate DoD offices standardize special access administrative forms; obtain appropriate approval for all DoD special access program forms; develop a protective marking to restrict distribution of special access unclassified information to the special access community; and develop guidance for the use, control, and accountability of information that requires the protective markings for inclusion in the appropriate DoD guidance (Finding B).

Management Comments. We received comments on the draft of this report from the Director, Special Programs, Office of the Under Secretary of Defense for Acquisition and Technology; the Deputy to the Under Secretary of Defense for Policy for Policy Support; the Chief, Technology Management Office, Army Staff; and the Director, Security and Special Program Oversight, Office of the Secretary of the Air Force. The Deputy to the Under Secretary of Defense for Policy for Policy Support concurred with all recommendations and stated that selected portions of the DoD Overprint to the Supplement, issued January 14, 1998, respond directly to several of the recommendations addressed in this report. The Army nonconcurred with the draft report recommendation to revise its regulation to correlate Army special access program categories with DoD special access program categories for waived, unacknowledged and acknowledged, but it stated that it would issue appropriate guidance. The Air Force comments did not specifically address the recommendation that it use the suggested menu of options that the Director, Special Access Program Coordination Office, established to standardize the Supplement's protective options within each special access program category. Part I of this audit report contains discussion of management's comments. Part III of the report provides the complete text of management comments.

Audit Response. Management comments to the draft report were generally responsive. We revised the draft recommendation to the Army to incorporate its proposed alternative action for issuing guidance to Army special access programs categorizing them as waived, unacknowledged and acknowledged. In response to the final report, we ask that the Air Force specifically comment on the recommendation concerning standardizing the Supplement's protective options within each special access program category by May 11, 1998.

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objective	4
Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement	5
Finding B. Administrative Standardization Among DoD Special Access Programs	18
Part II - Additional Information	
Appendix A. Audit Process	
Scope	32
Methodology	32
Management Control Program Review	33
Appendix B. Summary of Prior Coverage	34
Appendix C. Glossary of Supplemental Program Access Request Forms	36
Appendix D. History of the National Industrial Security Program Operating Manual Supplement	37
Appendix E. Text Differences Relating to Secret Accountability and Engineering Notebooks	39
Appendix F. Report Distribution	41
Part III - Management Comments	
Under Secretary of Defense for Acquisition and Technology Comments	44
Deputy to the Under Secretary of Defense for Policy for Policy Support Comments	47
Department of the Army Comments	50
Department of the Air Force Comments	52

Part I - Audit Results

~~FOR OFFICIAL USE ONLY~~

Audit Background

Special Access Programs. A special access program (SAP) is any program designed to control access, distribution, and protection of sensitive information in a manner beyond those normally used to protect classified information of a similar classification level. DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997, which implemented Executive Order 12958, "Classified National Security Information," April 17, 1995, describes the following criteria for establishing a SAP:

Any DoD program or activity as authorized by Executive Order 12958 . . . employing enhanced security measures exceeding those normally required by DoD 5200.1-R for information at the same classification level shall be established, approved, and managed as a DoD SAP. Examples of such enhanced security measures include the following: use of any special terminology, including code words, other than an unclassified nickname, to identify or control information dissemination; personnel security investigative or adjudicative requirements more stringent than those required for a comparable level of classified information; specialized non-disclosure agreements; exclusion of classified contract (use of carve-out); or a centralized billet system to control the number of personnel authorized access.

Executive Order 12958 states that, unless otherwise authorized by the President, only the Secretaries of State, Defense, and Energy and the Director of Central Intelligence, or the principal deputy of each, may create a SAP.

The National Industrial Security Program. Executive Order 12829, "National Industrial Security Program," January 1993, establishes the National Industrial Security Program as a single, integrated, and cohesive industrial security program to protect classified information within the Federal Government. In February 1994, the Joint Security Commission concluded that obsolete security standards and inconsistent program-specific applications caused problems inherent to SAPs, and the Joint Security Commission recommended a single set of standards to protect classified information. In response to the Executive order, the Deputy Secretary of Defense issued DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), in January 1995. It provides standardized requirements for the protection of classified information at the baseline protective level and also at enhanced and SAP protective levels. The Under Secretary of Defense for Policy issued DoD Manual 5220.22-M-Supplement 1, "National Industrial Security Program Operating Manual Supplement," in February 1995. The DoD NISPOM Supplement provides additional requirements and optional enhancements to protect information used in SAPs and SAP-type compartmented efforts. Appendix D provides a detailed description of the history of the NISPOM and the NISPOM Supplement.

Defense SAP Oversight. DoD Directive O-5205.7, "Special Access Program (SAP) Policy," reissued on January 13, 1997, established the SAP Oversight Committee. The SAP Oversight Committee is responsible for ensuring DoD compliance with SAP regulations. On January 13, 1997, the Deputy Secretary of Defense amended DoD Directive O-5205.7 to include the new requirements of Executive Order 12958, "Classified National Security Information," April 17, 1995. Executive Order 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

On January 5, 1994, the Deputy Secretary of Defense approved a plan to improve the management of SAPs throughout DoD. The plan clarified the procedures to establish, disestablish, and modify DoD SAPs, and expanded the responsibility and oversight role of the SAP Oversight Committee to include annual review of all DoD SAPs to validate continued SAP status. The plan also established the SAP Coordination Office as the single, centralized SAP management office within DoD to assist the SAP Oversight Committee and to serve as the DoD focal point on SAP matters with Congress and other Government agencies. The Director, Special Programs, Office of the Under Secretary of Defense for Acquisition and Technology, is the Director of the SAP Coordination Office. The Office of the Under Secretary of Defense for Policy develops overall security policy for SAPs. The Director for Special Programs, Office of the Deputy to the Under Secretary of Defense for Policy for Policy Support, is the Deputy Director of the SAP Coordination Office.

SAP Central Offices. Each Military Department has a SAP central office for coordinating SAP administration and oversight. The central offices for the Military Departments include the Chief, Technology Management Office, Army Staff (the Army SAP central coordinating office); the Director, Special Programs Division, Chief of Naval Operations (the Navy SAP central coordinating office); and the Director, Security and Special Program Oversight, the Office of the Secretary of the Air Force (the Air Force SAP central coordinating office). The responsibilities of the central offices are to:

- submit requests for establishment, annual review, and termination of their SAPs;
- exercise internal oversight and inspection programs for their SAPs;
- conduct an annual review of each SAP and its documentation; and
- establish adequate management controls and safeguards that include ensuring the appointment of a SAP security manager for each SAP.

Audit Objective

The overall audit objective was to evaluate areas to improve the efficiency and effectiveness of special access program security policies, procedures, and practices. The Chairman of the Special Access Program Oversight Committee's Senior Review Group requested that this audit validate the degree to which DoD was implementing the NISPOM Supplement. Specifically, we reviewed the efficiency and effectiveness of DoD Components' implementation of the NISPOM Supplement and the adequacy of special access administrative processes and forms. The audit also evaluated the adequacy of the management control program as it applied to the audit objectives. Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs," February 10, 1998, contains our review of the timeliness and consistency of the program access process and the need for program-specific security applications. Refer to Appendix A for a discussion of the scope, methodology, and review of the management control program. Appendix B discusses prior audit coverage related to the objectives.

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

The DoD special access community did not fully and effectively implement the NISPOM Supplement. The situation existed because the implementing guidance was not specific, and each DoD Component interpreted the NISPOM Supplement differently and took different steps to implement it. As a result, DoD Components provided their SAP contractors with redundant and conflicting security guidance. Consequently, contractors with multiple SAPs were unable to establish efficient security-related business processes within their facilities.

Policy for NISPOM Supplement Implementation Within DoD

DoD issued two memorandums to implement the NISPOM Supplement. The Under Secretary of Defense for Policy first directed implementation of the NISPOM Supplement in his memorandum, "Implementation of the National Industrial Security Program Operating Manual," June 14, 1995. The memorandum states that ". . . existing security requirements for DoD SAPs should be repromulgated in the form of an overprinted supplement . . ." within 120 days. Because implementation proceeded slowly, the Under Secretary of Defense for Policy and the Under Secretary of Defense for Acquisition and Technology issued a second memorandum, "Implementation of the National Industrial Security Program Operating Manual (NISPOM) Supplement," on August 20, 1996. The memorandum directs all DoD Components to immediately implement the NISPOM and the NISPOM Supplement on all new DoD contracts. The memorandum also requires all program offices to review existing DoD contracts for SAPs to determine the cost-effectiveness of implementing the NISPOM Supplement in relation to existing security requirements.

To facilitate implementation of the NISPOM Supplement and to encourage standardization of SAP security requirements, the Director, SAP Coordination Office, issued a memorandum, "Categorization of DoD Special Access Programs (SAPs)," October 15, 1996. The memorandum requests the DoD Components to categorize SAPs as acknowledged, unacknowledged, or waived,

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

based on the level of protection within each program. The memorandum then suggests which of the 45 NISPOM Supplement protective options to apply to each of the four levels¹ of SAPs.

DoD issued further guidance on categorizing SAPs in DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997. The instruction implements DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997, and disseminated policy, assigned responsibilities, and prescribed procedures for implementation and use in the management, administration, and oversight of all DoD SAPs. The instruction defines the three categories of DoD SAPs as follows:

Acknowledged SAP. An acknowledged SAP is a program of which the general public may know the existence and purpose, but for which its details, technologies, materials, and techniques remain classified, as dictated by its vulnerability to exploitation and the risk of compromise.

Unacknowledged SAP. An unacknowledged SAP is a program known only to a limited number of individuals; its purpose is protected as special access; and its details, technologies, materials, and techniques remain or are classified, as dictated by its vulnerability to exploitation and the risk of compromise.

Waived SAP. A waived SAP is an unacknowledged SAP to which an extremely limited number of individuals have access as required by statutory authority of Title 10, United States Code, Section 119e. The unacknowledged SAP protections also apply to waived SAPs.

Efforts of DoD Components to Implement the NISPOM Supplement

As of August 1997, only the Army had fully implemented the NISPOM Supplement by modifying all applicable SAP contracts and revising the related security procedures guides. Navy contracting officers had modified only 76 percent of its applicable SAP contracts, and the Air Force did not know how many contracts that it had modified. Although the June 1995 and August 1996 policy memorandums directed immediate implementation of the NISPOM Supplement, both memorandums and the NISPOM Supplement allowed the DoD Components flexibility in determining how to implement them. The guidance also did not clarify the ways that certain security options should apply

¹The four levels are: 1 - waived, 2 - unacknowledged, and 3 and 4 - acknowledged. Both Level 3 and Level 4 allowed baseline supplement protections. However, Level 3 also allowed the use of Director of Central Intelligence Directives as the guidelines for facility protection and personnel standards, and limited application of operational security measures.

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

to contractors. Without more specific guidance, each DoD Component took about a year and a half to develop its own implementing guidance. As a result, DoD Components delayed full implementation of the NISPOM Supplement, and contractors were subject to redundant implementing instructions and unclear operating requirements.

Army Implementation Efforts. The Army SAP central coordinating office attempted to implement the NISPOM Supplement consistently within Army SAPs. The Army SAP central coordinating office first attempted to implement the NISPOM Supplement by issuing a memorandum, "NISPOM Supplement," November 1995, to contracting officers. The memorandum directed contracting officers to modify existing SAP contracts by issuing revised DD Forms 254, "Contract Security Classification Specification." The memorandum also allowed program security managers to choose the options to apply to each SAP.

To provide program security managers more specific guidance on selecting options, the Army SAP central coordinating office drafted template guides for Category II and Category III SAPs, based on the menu of options outlined in the October 1996 memorandum. The Army SAP central coordinating office issued the template guide in December 1996 but rescinded it in February 1997. Program security managers suggested that revising existing security procedures guides to include the applicable options would be more efficient and less confusing than issuing separate guides.

Although the October 1996 memorandum requested DoD Components to categorize SAPs as acknowledged, unacknowledged, and waived, the Army SAP central coordinating office continued to categorize its SAPs as Category I, II, or III, as defined by Army Regulation 380-381(C), "Special Access Programs," January 4, 1993. While similar, Army Categories I, II, and III did not directly correspond to the DoD categories of acknowledged, unacknowledged, and waived. The Army terminology was, therefore, inconsistent with that of DoD, and the Army did not revise its regulation to conform to DoD guidance. The Army should issue guidance to Army SAPs categorizing its SAPs as waived, unacknowledged, or acknowledged, so that the programs can correlate the Army Categories I, II, and III security enhancements with the DoD SAP protective levels.

As a final measure to standardize the selection of security options and to implement the NISPOM Supplement, the Army SAP central coordinating office issued a memorandum, "Security Protective Levels and Menu of Options for NISPOMSUP [NISPOM Supplement]," April 7, 1997, to program security managers and contracting officers. The memorandum directs program security managers to implement the NISPOM Supplement by modifying contracts by May 30, 1997, and revising program security guides by July 31, 1997. The memorandum also outlines the security options to apply to each category of Army SAP. However, because the memorandum directs program security managers to apply the Two-Person Integrity rule to waived SAPs only, the memorandum conflicts with Army Regulation 380-381(C), which requires the Two-Person Integrity rule for all Army SAPs. To resolve the conflict, the

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

Army SAP central coordinating office issued a universal waiver of the Two-Person Integrity rule for Army Category II and III SAPs on April 23, 1997. The Army SAP central coordinating office revised Army Regulation 380-381(C) to reflect the NISPOM Supplement requirement and will issue the revised regulation in March 1998. As of August 1997, the Army SAP central coordinating office reported that program offices revised all Army SAP contracts and security program guides.

Navy and Air Force Joint Implementation Efforts. The Navy and the Air Force decided to develop and issue amplifying guidance before modifying applicable contracts. In response to the June 1995 memorandum, the Navy and the Air Force jointly developed the "Air Force/Navy Special Access Program Implementor" (the Joint Implementor), April 1996, to standardize procedures for NISPOM Supplement implementation and security options. Although the Navy and the Air Force coordinated to develop joint guidance, the Joint Implementor had Military Department-specific sections. In addition, the Joint Implementor was ambiguous and different than the NISPOM and the NISPOM Supplement.

The DoD contractors expressed concern about conflicting guidance in Navy and Air Force SAPs because the NISPOM eliminates the document accountability for Secret material, and the NISPOM Supplement lacks clear guidance on the accountability of engineering notebooks. The Navy and the Air Force in the Joint Implementor also eliminated accountability for Secret material but required contractors to record Secret material at receipt and dispatch. In addition, the Navy waived the document control requirement for Secret SAPs. The NISPOM Supplement states that contractors should mark engineering notebooks with the highest classification but does not mention accounting for the notebooks. In the Joint Implementor, the Navy and the Air Force both require contractors to account for working papers within 90 days from the date of their origin. The contradictions raise questions such as the following: How can a contractor account for Secret engineering notebooks when they were not received or dispatched? Does the 90 days from the date of origin begin after the start of the notebook or after the first Secret entry? In addition, for engineering notebooks, the Navy refers to "Secret" codewords in waived programs, and the Air Force refers to "classified." As a result, individual programs interpreted the NISPOM and NISPOM Supplement differently, creating confusing and burdensome guidance for contractors. See Appendix E for the specific conflicting text.

Navy Implementation Efforts. The Navy attempted to implement the NISPOM Supplement consistently within its SAPs. Specifically, the Navy categorized its SAPs as acknowledged, unacknowledged, and waived. The Navy SAP central coordinating office used the Joint Implementor as a basis to develop separate standardized program security guides for each SAP category. Each program security guide was an "overprint" of the NISPOM Supplement, meaning that it contained the contents of the NISPOM Supplement and

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

identified the security options and procedures required for that SAP category. The options in the program security guides were similar to the menu of options provided in the October 1996 memorandum.

Beginning in August 1996, the Navy SAP central coordinating office distributed copies of the interim program security guides to contractors for review and comment. At that time, the Navy SAP central coordinating office also requested the contractors to determine the cost impact of implementing the NISPOM Supplement. After the contractors reported that implementing the NISPOM Supplement would not have a cost impact, the contracting officers modified applicable contracts to require use of the program security guides. As of August 1997, Navy contracting officers had modified 76 percent of the applicable Navy SAP contracts.

Air Force Implementation Efforts. The Air Force did not implement the NISPOM Supplement consistently within its SAPs. Although the Air Force categorized its SAPs as acknowledged, unacknowledged, and waived, as requested in the October 1996 memorandum, it did not accept the Office of the Secretary of Defense Special Access Program Coordination Office recommended menu of options. Rather, the Air Force SAP central coordinating office used the Joint Implementor as a basis to develop the "Air Force Special Access Program Security Directive," February 28, 1997. However, the Air Force SAP Security Directive allows each program security officer to determine which options to apply to individual SAPs based on security risk and to develop a program-specific program security directive for each SAP. Nevertheless, the Air Force SAP central coordinating office did not provide guidance or training to program security officers on how to choose the options or implement the Air Force SAP Security Directive. Finally, contractors were not able to determine cost impact, as requested in the August 1996 memorandum, without knowing which options the program security officers selected for each SAP.

On October 31, 1996, the Director for Special Programs, Office of the Assistant Secretary of the Air Force (Acquisition), issued a memorandum to Acquisition SAP offices directing them to implement the NISPOM Supplement. The memorandum also provided general guidance on how to implement the NISPOM Supplement until the Air Force central coordinating office issued the Air Force SAP Security Directive. As of September 1997, the Air Force SAP central coordinating office had not established target dates for implementing the NISPOM Supplement and did not know how many contracts the Air Force had modified. The Air Force planned to modify contracts as they expire. In addition, the Air Force central coordinating office did not address operational and intelligence SAPs until it issued the Air Force SAP Security Directive. The section "DoD Implementer" in this finding explains Defense initiatives that will help to resolve the Air Force situation.

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

DoD Implementation Guidance for the NISPOM Supplement

National and DoD policy allowed the DoD Components flexibility in choosing the method to implement the NISPOM Supplement. For example, the opening paragraph of the NISPOM Supplement states:

Any Department, Agency, or other organizational structure *amplifying instructions* will be inserted immediately following the applicable security options selected from the NISPOMSUP [NISPOM Supplement]. This will facilitate providing a contractor with a supplement that is *overprinted* with the options selected. (emphasis added)

The Executive Agent of the NISPOM Supplement intended the implementing agencies to provide amplifying guidance and training to their components. However, because of the stated need for flexibility by the DoD Components, the Deputy to the Under Secretary of Defense for Policy for Policy Support did not specify exactly how the terms “amplifying instructions” or “overprint” would apply within DoD. In addition, neither the June 1995 memorandum nor the August 1996 memorandum directed the DoD Components to uniformly implement the NISPOM Supplement. Without specific DoD guidance to uniformly implement the NISPOM Supplement or formal training on how to apply the options, DoD Components interpreted the NISPOM Supplement differently and took different steps to implement it.

Multiple Security Guidance

Executive Order 12829 requires DoD to develop the NISPOM Supplement as the single Government regulation to protect classified information within SAPs. However, because of the different interpretations of the NISPOM Supplement and different implementing efforts, the Military Departments still subjected the contractors who had more than one SAP to multiple security guidance. Table 1 shows that a contractor with at least one SAP from each Military Department would have a minimum of nine types of guidance. The amount of guidance increased with the number of programs within a contractor facility because the Army and the Air Force required program-specific guidance, and the Navy required separate guidance for each category of SAP.

**Finding A. Implementation of the National Industrial Security Program
Operating Manual Supplement**

**Table 1. Security-Related Guidance Required at a Contractor Facility
With at Least One SAP per Military Department**

<u>Type of Security Guidance</u>	<u>Army</u>	<u>Navy</u>	<u>Air Force</u>	<u>Amount at Facility</u>
NISPOM	X	X	X	1
NISPOM Supplement	X		X	1
Security Procedures Guide for each program	X			1
Program Security Guide for each category ¹		X		1
Joint Implementor ²			X	0
Air Force SAP Security Directive			X	1
An Appendix for each Program			X	1
Standard operating procedures for each program	X	X	X	3
Total for Contractor Facility				9

¹The SAP categories are acknowledged, unacknowledged, and waived.

²Although not issued to SAP contractors, the Air Force referenced the Joint Implementor in the Air Force SAP Security Directive.

Duplicate Standard Operating Procedures for a Contractor Facility

The first of the 45 options in NISPOM Supplement, Section 1-201, states:

The CPSO [Contractor Program Security Officer] may be required to prepare a comprehensive SOP [standard operating procedure] to implement the security policies and requirements for each SAP. When required, SOPs will address and reflect the contractor's method of implementing the PSG [Program Security Guide]. Forward proposed SOPs to the PSO [program security officer] for approval. SOPs may be a single plan or series of individual documents each addressing a security function. Changes to the SOP will be made in a timely fashion, and reported to the PSO as they occur.

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

The option applies to Levels 1, 2, and 3. The standard operating procedures are similar to standard practice procedures formerly required by the Industrial Security Manual. The Navy included the standard operating procedure requirement in all three of its program security guides, and the Air Force included the requirement in the Air Force SAP Security Directive. The standard operating procedures are a program-specific requirement at each facility; however, acquisition streamlining encourages facilitywide standardization. Therefore, the standard operating procedure should not be a program-specific requirement that causes the contractor to repeatedly obtain approval of the same basic standard operating procedure; it should be a facilitywide standard operating procedure that, once approved, is applicable to all SAPs located at that facility. The Single Process Initiative, discussed in the following section to this report, is a means of making the standard operating procedures facilitywide.

Use of the Single Process Initiative to Implement the NISPOM Supplement

On December 8, 1995, the Secretary of Defense and Under Secretary of Defense for Acquisition and Technology announced implementation of the DoD Single Process Initiative (the Initiative). The Under Secretary of Defense memorandum, "Single Process Initiative," December 8, 1995, directs the administrative contracting officer, the single point of contact for the effort, to encourage contractors to prepare and submit concept papers describing practices that will permit uniform, efficient, facilitywide management and manufacturing systems. The administrative contracting officer will coordinate with the contractor to convert existing contracts to the most efficient process. The memorandum also designates the Commander, Defense Contract Management Command, as the focal point for implementing the Initiative within DoD and as the facilitator to coordinate the change process.

The DoD Component SAPs could use the Initiative, implemented through contractor-proposed block changes, to modify SAP contracts and to more effectively and efficiently implement the NISPOM Supplement. The Secretary of Defense December 6, 1995, memorandum, "Common Systems/ISO-9000/-Expedited Block Changes," states that ". . . [because] it is generally not efficient to operate multiple, government-unique management and manufacturing systems within a given facility, there is an urgent need to shift to facilitywide common systems on existing contracts" The Secretary of Defense memorandum directed DoD Components to make block changes to the management and manufacturing requirements of existing contracts on a facilitywide basis. It also required DoD Components to unify management and manufacturing requirements within a facility wherever such changes are technically acceptable to the Government.

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

The DoD should encourage SAP contractors to propose block change modifications to implement the NISPOM Supplement and standardize operating procedures to the extent possible at contractor facilities with multi-Agency, multi-category DoD SAPs. In his September 26, 1996, speech to the Strategic Systems Industrial Symposium, the Under Secretary of Defense for Acquisition and Technology illustrated the significance of the block change process for modifying management and manufacturing processes at contractor facilities. The Under Secretary of Defense for Acquisition and Technology stated that “. . . a single block change modification impact[ed] 884 contracts at 16 separate Raytheon facilities.” As of July 1997, contractors submitted 977 proposals for block changes at 206 DoD-wide contractor facilities. Of the 977 proposals submitted, DoD approved 510 proposals, with an estimated annual cost avoidance of \$75.3 million.

DoD Implementer

The Deputy to the Under Secretary of Defense for Policy for Policy Support is currently developing the “DoD Implementer to the NISPOMSUP [NISPOM Supplement]” (the DoD Implementer). The DoD Implementer will outline which of the 45 NISPOM Supplement protective options will apply to acknowledged, unacknowledged, and waived SAPs and will provide guidance on how to implement the protective options within DoD SAPs. Consistent with Executive Order 12958 and other SAP policies, the DoD Implementer will allow the DoD Components to rescind selected options if they do not believe that a SAP warrants the enhancements; that is, to “waive down” options. However, if the DoD Components believe that a SAP warrants protection above the specified SAP protective level, they must obtain approval from the DoD SAP Oversight Committee to “waive up” options.

Conclusion

Contrary to the original intent of the NISPOM Supplement, each DoD Component interpreted the NISPOM Supplement differently and took different steps to implement it. As a result, DoD Components issued multiple documents and redundant implementing instructions. Providing standardized guidance to contractors for acknowledged, unacknowledged, and waived SAPs would eliminate multiple and redundant documents and would allow contractors to develop a single, facilitywide set of standard operating procedures for each SAP category. Standardized guidance should effectively reduce contract overhead cost and would foster security risk management rather than risk avoidance. In addition, standardizing SAP security guidance would be a positive step toward achieving the directive of the Secretary of Defense to shift to facilitywide common business practices for contractors. Although the audit primarily

Finding A. Implementation of the National Industrial Security Program Operating Manual Supplement

focused on SAPs managed by the Military Departments, DoD senior SAP officials stated that the problems identified were also applicable to the Defense agencies.

DoD Components should consider security a function of the management process and should encourage contractors to take advantage of the Initiative by proposing block changes to facilitate implementation of uniform and efficient facilitywide security processes. Block changes proposed and approved would standardize operating procedures for contractors that have multiple SAPs within their facilities, which in turn would increase efficiency and effectiveness. A July 1997 DoD Industrial Security Letter (ISL 97-1) encouraged SAP contractors to identify opportunities for standardizing SAP security requirements and provided general guidance for submitting proposals for block changes. However, because of the sensitivity of operating procedures within SAP contractor facilities, the Deputy to the Under Secretary of Defense for Policy for Policy Support, in coordination with the Commander, Defense Contract Management Command, should develop appropriate procedures for handling block changes within contractor facilities that have multiple SAPs.

Management Comments on the Finding and Audit Response

Department of the Air Force Comments on Implementing the NISPOM Supplement. The Director, Security and Special Program Oversight, commented that the Air Force co-authored the proposed NISPOM Supplement Overprint and, therefore, intends to follow the guidance. Because the Overprint closely resembles the Joint Implementor, the Air Force stated that it has used the NISPOM Supplement menu of options since its inception. In his comments, the Director, Security and Special Program Oversight, also stated that the audit report, in an attempt to standardize, prescribed administrative efficiencies that were detrimental to overall program security and program management. He noted that the report correctly states that Air Force program security officers are allowed to tailor program security through the selection of NISPOM Supplement options based on security risk to the program. However, he stated that contrary to the report findings, the Air Force believes that security is paramount in developing and executing a SAP, as opposed to relieving Government and contractor personnel of minor administrative tasks. The Director, Security and Special Program Oversight, concluded that efficient and effective SAP security is gained by implementing those NISPOM Supplement options that appropriately address the threat of a program and not by implementing a prescribed set of options geared to a particular SAP category.

Audit Response. Although the Air Force co-authored the Joint Implementor, the Air Force was not a signatory on the final version that standardized, within the Navy, the NISPOM Supplement options by SAP category: waived, unacknowledged, and acknowledged. In contrast, the Air Force developed and issued the Air Force Program Security Directive, which required its SAP contractors to refer to the NISPOM, the NISPOM Supplement, the Joint

**Finding A. Implementation of the National Industrial Security Program
Operating Manual Supplement**

Implementor, and the program-specific security guides to obtain clarification on specific security issues. Therefore, contractor program security officers had multiple documents to maintain and review, and the number of documents exponentially increased with the number of Air Force SAPs that the contractor had within a single location. The proposed DoD Overprint, when implemented, will standardize the NISPOM Supplement options by SAP category. The Overprint will allow DoD Components to rescind selected options if they do not believe that a SAP warrants the enhancements; that is, to “waive down” options. However, if the DoD Components believe that a SAP warrants protection above the specific SAP protective level, they must obtain approval from the DoD SAP Oversight Committee to “waive up” options. In addition, the Air Force comments regarding program security officers using threat as a basis to tailor security enhancements is inconsistent with our discussions with Air Force program security officers. Generally, program security officers could not support any security enhancement based on the threat to the SAP. Security enhancements were generally imposed to protect the technologies and sensitive information related to a SAP.

Recommendations, Management Comments, and Audit Response

Revised Recommendations. As a result of management comments, we revised draft Recommendation A.3. to the Chief, Technology Management Office, Army Staff, to incorporate the alternative solution of the Army to issue guidance to Army programs categorizing its special access programs as waived, unacknowledged, or acknowledged so that the programs can interpret guidance from DoD.

A.1. We recommend that the Director for Special Programs, Office of the Deputy to the Under Secretary of Defense for Policy for Policy Support, who also serves as the Deputy Director, Special Access Program Coordination Office, in coordination with DoD Components:

a. Finalize and issue the DoD Implementer to the National Industrial Security Program Operating Manual Supplement to provide implementing guidance for the 45 protective options for special access programs.

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments. The Deputy to the Under Secretary of Defense for Policy for Policy Support concurred with the recommendation and stated that DoD issued the NISPOM Supplement Overprint in January 1998. The SAP Security Standards Working Group developed the Overprint, which contains uniform security guidance for all DoD SAPs. The Deputy to the Under Secretary of Defense for Policy for Policy Support commented that the Overprint will facilitate reciprocity and enhance standardization within the DoD SAP community.

**Finding A. Implementation of the National Industrial Security Program
Operating Manual Supplement**

b. Provide guidance to special access program contractors as a part of the issuance of the implementation above, explaining what a reasonable period of time is for retrieval and disposition of nonaccountable classified documents and when contractors should control and consider engineering notebooks accountable as classified documents.

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments. The Deputy to the Under Secretary concurred, stating that the Overprint provides guidance on the retrieval and disposition of nonaccountable documents, based on the type of information as opposed to the level of classification. He stated that the Overprint contains a matrix that displays different types of classified and unclassified information, the retention period of the information, and disposition and destruction guidance. The Deputy to the Under Secretary also commented that the Overprint, in paragraph 5-206, provides detailed guidance on the accountability, marking, reproduction, and retention of engineering notebooks.

A.2. We recommend that the Deputy to the Under Secretary of Defense for Policy for Policy Support, in coordination with the Commander, Defense Contract Management Command, develop policy to formally implement the Single Process Initiative within DoD special access programs to facilitate uniform and efficient facilitywide security processes at contractors that work on special access programs.

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments. The Deputy to the Under Secretary of Defense for Policy for Policy Support concurred with the recommendation and stated that DoD Industrial Security Letter 97-1, July 1997, encouraged contractors to identify opportunities for implementing the Initiative. Furthermore, he commented that the office would continue to work with the appropriate organizations to explore additional ways to implement the Initiative within DoD SAPs.

A.3. We recommend that the Chief, Technology Management Office, Army Staff, issue guidance to Army special access programs categorizing its special access programs as waived, unacknowledged, or acknowledged so that the programs can correlate the Army Categories I, II, and III security enhancements with the DoD guidance.

Army Comments. The Chief, Technology Management Office, Army Staff, nonconcurrent with the draft report Recommendation A.3., which stated that the Army should revise Army Regulation 380-381(C), "Special Access Programs," January 4, 1993, to specifically correlate Army SAP Categories I, II, and III with the DoD SAP categories. He stated that revising an Army regulation was not the most effective method to implement evolving guidance. He stated that the DoD SAP Security Working Group had not finalized the correlation among DoD SAP categories, the number of SAP sensitivity levels, and security enhancements available to each sensitivity level. He suggested that we reword the recommendation to state that the Army should publish guidance categorizing SAPs as waived, unacknowledged, or acknowledged. The guidance will

**Finding A. Implementation of the National Industrial Security Program
Operating Manual Supplement**

designate the appropriate DoD category for each Army SAP. The Chief, Technology Management Office, Army Staff, further stated that the Army compliance with the use of DoD categories is evidenced in the annual SAP report, because the Army identified SAPs by DoD category in that report.

Audit Response. In response to the Army comments on the draft report recommendation, we revised the recommendation. The Army comments are responsive to the revised recommendation. No further comments are needed from the Army.

A.4. We recommend that the Director, Security and Special Program Oversight, Office of the Secretary of the Air Force, use the suggested menu of options in the Director, Special Access Program Coordination Office, memorandum of October 15, 1996, to standardize National Industrial Security Program Operating Manual Supplement protective options within each special access program category.

Air Force Comments. The Director, Security and Special Program Oversight, concurred with comment on the audit finding, but he did not specifically comment on the recommendation.

Audit Response. In response to the final report, we request that the Air Force specifically address Recommendation A.4.

Finding B. Administrative Standardization Among DoD Special Access Programs

The DoD SAPs subjected the contractors that deal with multiple SAPs to inefficient, redundant, and unclear administrative requirements, including varying and duplicative SAP documents, storage requirements, other security-related processes, and protective markings. The inefficiency and redundancy existed because DoD and the Military Departments lacked standardized SAP administrative forms, processes, and protective markings. The inefficient and redundant requirements were burdensome and confusing to contractors, increased contractor overhead costs, and had the potential for delaying performance on SAP contracts.

Guidance on Administrative Documents and Protective Markings

Administrative Documents. Realizing the lack of standardization in SAP documents, the NISPOM Supplement Working Group developed 26 standardized SAP formats for inclusion in the NISPOM Supplement. However, the NISPOM Supplement Working Group did not publish the forms as part of the NISPOM Supplement because of the time required to obtain the Office of Management and Budget approval of the forms. Nevertheless, the Navy and the Air Force adopted the formats for use in Navy and Air Force SAPs. Before they started using the NISPOM Supplement formats, the Navy SAPs had standardized forms, and each Air Force SAP had developed its own local forms that required essentially the same information. Conversely, the Army did not adopt the SAP formats but continued to use forms approved by the Department of the Army as prescribed by Army Regulation 380-381(C), "Special Access Programs," January 4, 1993, and generated other forms on a SAP-by-SAP basis.

Protective Markings. DoD Pamphlet 5200.1-PH, "A Guide to Marking Classified Documents," April 1997, provides general guidance on security classification markings. The DoD used the guidance contained in Executive Order 12958, "Classified National Security Information," April 17, 1995, to revise language in the pamphlet. The pamphlet applies to all DoD Components. Protective markings alert holders to the presence of classified information. Protective markings also identify the exact information or portion that

Finding B. Administrative Standardization Among DoD Special Access Programs

needs protection; provides guidance for downgrading and declassifying; gives the reason for the initial classification decision; and warns the holders of any special access, controls, or safeguarding requirements.

In the following section, we describe conditions at 22 SAP program offices and 22 contractor facilities.

Administrative Documents, Processes, and Markings in SAPs

DoD did not develop standardized program access documents and other administrative security-related processes and documents. Therefore, contractor personnel working with multiple SAPs completed duplicative documents and met redundant security-related requirements. In addition, the lack of standardized protective markings for SAP documents required the purchase of various types of storage containers, some of which were very expensive.

Program Access. DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997, states that, for access to a DoD SAP, an individual must meet a need-to-know determination, have the requisite security clearance, meet any approved upgraded personnel security requirements for access, and clearly and materially contribute to the execution or oversight of the program. The minimum personnel security requirements for access are a final Secret clearance, with verification of the security requirements current within 5 years. To establish reciprocity, SAP-accessed personnel must have periodic investigations every 5 years to ensure that their security eligibility requirements are current. Access determinations for SAPs are an adjudicative function relating to a person's suitability for such access.

Within DoD, each Defense Component established the requirements for access to its SAPs. As a result, contractors that deal with multiple SAPs had to complete, process, and maintain multiple program access documents.

Program Access Requirements and Documents. The lack of standardized program access documents impeded access reciprocity within and among DoD SAPs. As a consequence, individuals requiring access to more than one SAP generally submitted a separate program access request (PAR) package to each SAP. Each Military Department SAP central coordinating office required the requesting organization to complete an access request document to justify an individual's access to one of its SAPs. In addition, each Military Department SAP central coordinating office also established different requirements for access to its SAPs. The Army has only a two-step process. The applicant must have a current collateral security clearance at the classification level of the SAP, and the requesting organization must complete DA Form 5749-R, "Request for Access," to justify the individual's need-to-know for access to the SAP.

Finding B. Administrative Standardization Among DoD Special Access Programs

In contrast, the Navy and the Air Force have a four-step process. First, like the Army, the individual must have a current collateral security clearance at the classification level of the SAP. Second, the requesting organization must complete and process a PAR package. The PAR package must include SAP Format 1, "Program Access Request (PAR)," and Standard Form 86, "Questionnaire for National Security Position." In addition, depending on the SAP access requirements, the PAR package will include the "Classified Program Security Questionnaire," the "Foreign Relative or Associate Interview," the "Personal Financial History Form," and the "Drug Questionnaire." Third, the Navy and the Air Force program security officers readjudicate to determine whether the individual meets the SAP security access eligibility requirements. Readjudication involves conducting a Defense Clearance and Investigations Index (DCII) check and reviewing all information in the PAR package. The Air Force SAPs require the requesting organization to obtain the DCII check and provide it as part of the PAR package. The fourth step for access to a Navy or Air Force SAP is the program manager's need-to-know determination.

Table 2 shows the various program access documents that each Military Department may require for access to its SAPs. See Appendix C for a description of the various supplemental PAR forms shown in Table 2.

Table 2. Program Access Request Documents

Document	Army	Navy	Air Force
Access Request Document ¹	Yes	Yes	Yes
Standard Form 86	No	Yes	Yes
Request for DCII Files Check	No	No ²	Yes
Classified Program Security Questionnaire	No	No	S ³
Foreign Relative or Associate Interview	No	S	S
Personal Financial History Form	No	S	S
Drug Questionnaire	No	S	S

¹ A required document to justify the need-to-know determination for access.
² The Navy obtains DCII information when the program security officer receives the PAR package. It does not require the requester to obtain DCII information before submitting the PAR package.
³ S = Sometimes, on a program-by-program basis.

Because the Military Department SAPs used different access request documents and had different access eligibility requirements, a person requiring access to more than one SAP had to complete separate program access documents and meet different access eligibility requirements for each SAP. The lack of standardization for SAP access impeded access reciprocity within and among DoD SAPs. Inspector General, DoD, Report No. 98-067, "Access Reciprocity

Finding B. Administrative Standardization Among DoD Special Access Programs

Between DoD Special Access Programs,” February 10, 1998, discusses in more detail the other problems associated with the lack of access reciprocity within and among Military Department SAPs.

Access to Multiple SAPs. Standardizing administrative documents would reduce contractor overhead charges because contractor employees requiring access to multiple SAPs would prepare fewer documents after their initial access to a SAP. In addition, standardized documents would reduce a contractor’s time for processing duplicative PAR packages and reduce requirements for storage containers.

Time Factor. The time to complete, process, and readjudicate a single PAR package generally is not excessive; however, the time to complete, process, and readjudicate duplicative PAR packages is excessive and costly for multiple accesses to SAPs. Generally, the Navy and the Air Force did not reciprocally acknowledge SAP security eligibility determinations adjudicated within and between their respective Military Departments. Also, although the Army established reciprocity within Army SAPs, Army access documents were not reciprocal with Navy and Air Force SAP access documents. As a consequence, contractor employees who required access to multiple SAPs within or between the Military Departments generally had to complete a separate PAR package to obtain access to each requested SAP.

Because contractor employees did not have access to the requested SAPs, employees charged their time to complete the PAR packages to an overhead account. An hour is the average time charged to overhead for reviewing and not changing a previously prepared Standard Form 86. When contractors totaled the time it takes for employees to complete multiple PAR packages for access to several SAPs, the overhead cost to the contractor and the Government can be considerable. Five contractors tracked multiple accesses to SAPs and provided the numbers shown in Table 3. To determine the number of duplicative accesses, we allowed one access per individual and subtracted the number from the number of multiple accesses granted an individual. For those five contractors, 7,119 employees completed 18,030 duplicative PAR packages. In addition, contractor security personnel processed, and Navy and Air Force Program Security Officers readjudicated, the same number of duplicate PAR packages.

Finding B. Administrative Standardization Among DoD Special Access Programs

Table 3. Contractor Employees Accessed to Multiple SAPs That Required Completion, Processing, and Readjudication of Duplicative PAR Documents			
Contractor	Number of Employees (a)	Number of Accesses (b)	Duplicative Accesses (c)
A ²	300	2,500	2,200
B ²	1,244	3,774	2,530
C ²	2,208	6,629	4,421
D ²	3,087	10,997	7,910
E ²	<u>280</u>	<u>1,249</u>	<u>969</u>
Total	7,119	25,149	18,030

Backlogs From Duplicative PAR Packages. Duplicative processing of PAR packages caused a backlog within the security offices of Contractor F². At one of its facilities with multiple SAPs, security personnel at Contractor F² stated that the Military Departments required 18 different documents to process their DoD SAPs. The contractor's central PAR facility processed approximately 150 PAR packages each month. Security personnel at Contractor F² estimated that approximately one-third of the PAR packages that were processed were duplicates and the duplicates caused a backlog. As a result, employees did not receive timely access to SAPs.

Storage Requirements Because of Duplicative and Different Classification Levels of PAR Packages. Contractors had to acquire various types of storage containers because each SAP within the Military Departments required contractors to maintain copies of all administrative documents for each access to the SAP. In addition, the lack of reciprocity among DoD SAPs and the lack of standardized PAR packages and classification levels required contractors to acquire various and costly storage containers to maintain multiple and duplicative program access documents. Contractor security officers processed and maintained copies of duplicative PAR packages for individuals accessed to multiple SAPs because the Military Departments did not generally acknowledge reciprocity within and among their SAPs.

² Real names of the contractors are not used in the report for security reasons.

Finding B. Administrative Standardization Among DoD Special Access Programs

In addition, the Military Department SAPs did not have standardized protective markings for the PAR forms. Because of the different classification levels of the PAR forms, contractors acquired various types of storage containers, and some of those containers were more costly than others. For example, the Army uses the unclassified program nickname on its DA Form 5749-R and allows the document to be stored in filing cabinets within the program area because the Army classifies the document as "For Official Use Only." In contrast, the Navy uses the SAP Secret codeword on the PAR form, requires the document to be marked "Secret/Special Access Required," and requires the PARs to be stored in a General Services Administration-approved security container located within the program area. Like the Army, the Air Force uses the unclassified nickname in the PAR. However, because the justification for need-to-know may include program-specific information, the Air Force classifies the PAR as "Confidential/Special Access Required" and allows it to be stored in a lockbar cabinet located within the program area. Because of the varying storage requirements of the Military Department SAPs and associated costs, Contractor B obtained approval from its Navy and Air Force SAPs to establish a central security office. The central security office allowed the contractor to centralize storage of administrative documents and thereby eliminate the storage of duplicative documents.

Sharing of PAR Package Information. In response to a working draft of this report, a SAP official expressed concern about sharing PAR package information between acknowledged and unacknowledged SAPs. Generally, acknowledged and unacknowledged SAPs do not share information because of the sensitivity of unacknowledged SAP information. Our evaluation of the program access requirements and documents indicated that the access request document, the need-to-know justification, is the only document that would have program sensitive information that may require compartmentalization. Other supplemental PAR documents contain personnel-related information and do not require compartmentalization. Therefore, an individual requiring access to multiple unacknowledged SAPs should not complete multiple supplemental PAR documents. The individual should review and update supplemental PAR personnel information as necessary when requiring access to multiple SAPs. In Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs," February 10, 1998, we recommended that the SAP community develop a critical information update form for that purpose. The contractor security officer could maintain supplemental PAR documents and other administrative security documents in a centralized area in appropriate storage containers.

Other Administrative Requirements and Documents. Redundancy and lack of standardized forms also existed for other security-related administrative functions required by the Military Departments at SAP contractor facilities. For example, Military Department SAPs required their contractors to conduct multiple annual refresher security briefings. Also, the DoD SAP community did not use standardized forms to report foreign travel and foreign contacts and did not use standardized indoctrination and termination forms.

Finding B. Administrative Standardization Among DoD Special Access Programs

Annual Refresher Security Briefings. The Military Departments did not have a standardized document for reporting attendance at the annual refresher security briefing and did not generally require individuals accessed to multiple SAPs to attend only one annual refresher security briefing. Because Army SAPs did not have a standardized form to report annual security briefings, each SAP developed its own program-specific format. In contrast, both Navy and Air Force SAPs used SAP Format 17, "Refresher Training Record."

Although an individual accessed to multiple SAPs attended at least one refresher briefing, each SAP required separate attendance to a refresher briefing. Meeting that administrative requirement consumed valuable time, which reduced performance on the contracts and increased overhead cost to contractors. Contractor A, who had multiple SAPs within the same facility, realized the inefficiency of the current process and established one annual refresher briefing for those who were accessed to multiple SAPs. The contractor distributed a copy of the individual's training paperwork to each accessed SAP. On February 28, 1997, the Air Force issued the Air Force Special Access Program Security Directive, which allowed those who were accessed to multiple SAPs to attend only one annual security refresher briefing.

Foreign Travel and Foreign Contact Reporting. Standardized forms to report foreign travel and foreign contact did not exist within the DoD SAP community. The Army did not have standardized forms for reporting foreign travel and foreign contact; therefore, each program developed its own form. In contrast, Navy and Air Force SAPs used SAP Format 6, "Notification of Foreign Travel," and SAP Format 20, "Foreign Relative or Associate Interview." In addition, the lack of a focal point within DoD to receive and disseminate reports on foreign travel and contact required those who were accessed to multiple SAPs to report to each SAP program office. Because of the ineffective system of reporting, the potential existed that foreign travel and foreign contact would not be reported to all SAP program offices. Contractor A standardized reporting foreign travel within the facility by providing one briefing and copies of the signed travel form to the appropriate SAPs. Contractor A averaged 8 accesses for each person accessed to multiple programs (2,500 accesses divided by 300 individuals); therefore, the contractor eliminated about seven reporting requirements per person.

Standardized Indoctrination and Termination Forms. DoD did not standardize the indoctrination and termination forms that DoD Component SAPs use. The Army uses DA Form 5399-R, "Special Access Program Initial Security Briefing." The form specifies that an individual granted access to an Army SAP is subject to urinalysis testing. The Army uses DA Form 5401-R, "Special Access Program Security Termination Briefing," to terminate access to a SAP. Both the Navy and the Air Force use SAP Format 2, "Special Access Information Agreement," for both indoctrination and termination. In contrast, SAP Format 2 does not specify that an individual granted access to a Navy or Air Force SAP is subject to urinalysis testing.

Finding B. Administrative Standardization Among DoD Special Access Programs

The lack of standardized administrative security forms within the DoD SAP community has caused burdensome and conflicting requirements on SAP contractors. In addition, the multiple documents impeded the ability of SAP contractors to implement simplified facilitywide security processes to reduce overhead cost and to increase performance on SAP contracts.

To standardize SAP security-related forms within the national industrial community, the NISPOM Supplement Working Group developed several SAP formats. To expedite the issuance of the NISPOM Supplement, the working group did not obtain approval from the Office of Management and Budget to require SAP contractors to use those documents as forms. To achieve standardization, the Deputy to the Under Secretary of Defense for Policy for Policy Support should obtain the appropriate approval and make the SAP formats official DoD forms. The DoD SAPs may need to continue to use the formats while DoD officials proceed with the effort to obtain the Office of Management and Budget approval of the actual forms.

SAP Protective Markings. DoD did not have standardized protective markings for SAP information that requires restricted access but that is not Confidential, Secret, or Top Secret. The Navy and the Air Force used "Handle Via Special Access Channels Only" or "HVSACO" for page and paragraph markings. The Army does not acknowledge such a protective marking; however, Army programs were using operation-sensitive restrictive statements. The Army program offices recorded the restrictive statements only on the cover or the first page of the documents. As a consequence, the removal of the page having the restrictive statement negates the intent of the restriction.

If DoD SAPs had a standardized protective marking such as "FOR OFFICIAL USE ONLY/Not for Release Outside of the SAP Community," contractors and Government personnel could store unclassified program documents in a more cost-effective manner within the program area, rather than in General Services Administration-approved containers. Unnecessary use of higher classifications increases the requirement for costly General Services Administration containers and is in direct opposition to Executive Order 12958, which states that if the appropriate level of classification is in doubt, classify documents at the lowest level.

Although the need for standardized protective marking exists, DoD management must consider the potential for abuse. For instance, program offices could potentially put the restrictive protective marking on declassified SAP information to keep that information from the general public review. Therefore, the Director of Special Programs, Office of the Deputy to the Under Secretary of Defense for Policy for Policy Support, should develop guidance to include, as a minimum, the appropriate use of protective marking and conditions for controlling and accountability.

Use of Single Process Initiative to Standardize SAP Reporting Requirements. DoD SAPs could encourage contractors to use the Initiative to standardize SAP administrative functions within contractor facilities that have

Finding B. Administrative Standardization Among DoD Special Access Programs

multiple SAPs. The goal of the Initiative was to reduce contractor operating costs and achieve cost, schedule, and performance benefits for the Government by replacing multiple, Government-unique management and manufacturing systems with common, facilitywide systems.

Conclusion

Redundancy in special access, security-related processes impeded contractors in establishing good business practices. Redundancy occurred because the DoD SAP community did not standardize special access security administrative forms and functions. For example, Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs," states that individuals requiring access to multiple SAPs complete multiple PARs packages rather than complete an access update form. The lack of standardized security administrative forms and protective markings within SAPs placed a hardship on the SAP industrial base. As a consequence, the DoD SAP community presented itself to the industry base as separate disjointed entities rather than as a "single face to industry." Implementation of the recommendations in this report and Report No. 98-067, "Audit of Access Reciprocity Between DoD Special Access Programs," along with ongoing efforts in the SAP community, should lead to much more efficient and effective special access security-related processes within DoD and the industry.

Management Comments on the Finding and Audit Response

Office of the Under Secretary of Defense for Acquisition and Technology Comments on Readjudication. Although not required to comment, the Director, Special Programs, Office of the Under Secretary of Defense for Acquisition, stated that program security officers do not readjudicate an individual for access to a SAP, but instead, they revalidate the individual's suitability for access. He stated that the need for the revalidation will be mitigated when his office establishes common SAP adjudicative standards and adjudication training. However, the Director, Special Programs, added that there will always be a need to review the clearance and investigation information for currency to ensure that new information does not adversely impact an individual's suitability and eligibility for access to SAPs, which he calls "revalidation."

Audit Response. We believe that we were correct in calling the review of an individual's PAR package for access to SAPs a readjudication. As we view it, readjudication is a multi-tiered process performed by both the program security officer and SAP adjudicators. In the readjudicative process, the program security officer is restricted to making only affirmative determinations regarding an individual's security eligibility and suitability. The SAP central adjudicators make both affirmative and denial determinations for SAP access.

Finding B. Administrative Standardization Among DoD Special Access Programs

When an individual is nominated for SAP access, the program security officer reviews the PAR package to determine whether the person meets certain security eligibility and suitability criteria established specifically for the SAP as allowed by Executive Order 12968, "Access to Classified Information," August 4, 1995. The PAR package contains an individual's personnel security information, which is basically the same information used to adjudicate an individual's eligibility for access to collateral classified information and sensitive compartmented information. The program security officer may not deny access but does make affirmative access decisions. Should the PAR package identify potentially disqualifying information or issues, the package is forwarded to the SAP adjudicator for further review and an adjudicative decision.

The Department of the Army Comments on the Personnel Security Requirements for Access to SAPs. The Chief, Technology Management Office, commented that the purpose of the periodic reinvestigation is to maintain access eligibility and not to establish reciprocity. He stated that access determinations are based on a need-to-know once access eligibility is verified.

Audit Response. The rationale of the Army for the revision of the draft report is incorrect. Although the personnel security clearance must be current within 5 years for an individual to obtain access to a SAP, a current personnel security clearance is not always needed to maintain SAP access. Unless a special access-authorized organization tracks the currency of its personnel security clearances for continuous SAP access and requests a periodic reinvestigation, the Defense Security Service will not initiate a periodic investigation every 5 years unless an individual was seeking access to another SAP.

The Department of the Army Comments on the Use of the Access Request Forms. The Chief, Technology Management Office, stated that Table 2, "Program Access Request Documents," was misleading because it included the Access Request Document that is required for access to each SAP. The duplication, he noted, is in the number and types of supplemental documentation required for submittal along with the Access Request Document.

Audit Response. We added a footnote to Table 2 to indicate that the Access Request Document is a required document to justify the individual's need-to-know for access to a SAP.

The Department of the Air Force Comments on the Finding. The Director, Security and Special Program Oversight, stated that the forms used in the DoD Overprint were drafted by the Air Force and were predominantly derived from the Joint Implementer and the Air Force Program Security Directive. He added that contrary to the audit report, the Air Force implemented the NISPOM Supplement consistently within the Air Force, but not across the Levels I, II, and III Air Force SAPs. The Air Force comments assert that the audit report does not give conclusive evidence that efficiencies can be gained by categorizing SAPs and assigning NISPOM Supplement options to SAPs based on those categories. Additionally, the Air Force reiterated its position that program

Finding B. Administrative Standardization Among DoD Special Access Programs

security will remain most effective and efficient by tailoring security to the specific threats to the program. The Director, Security and Special Access Program Oversight, stated that the Air Force will continue to select options for each Air Force SAP based on the threat and that the concept reflects full adherence to the intent of the NISPOM Supplement and the DoD Overprint.

Audit Response. The finding gave examples of administrative inefficiencies that, when multiplied exponentially, increased the cost of administering security for DoD SAPs. Although security is an important issue in a SAP, the program security officer should consider risk management rather than risk avoidance and should consider ways in which security can be achieved in a uniform and cost-effective manner. As stated in our response to Finding A, generally program security officers could not support any security enhancements based on a the specific threat to the SAP.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Director of Special Programs, Office of the Deputy to the Under Secretary of Defense for Policy for Policy Support, who also serves as the Deputy Director, Special Access Program Coordination Office:

1. Review the special access program formats developed by the National Industrial Security Program Operating Manual Supplement Working Group and determine the formats that are necessary for DoD special access programs. For the necessary formats and any other forms used by the special access community, develop standardized forms for use in the DoD special access program community and obtain the appropriate approval of the forms. In the interim, use the appropriate formats developed by the National Industrial Security Program Operating Manual Supplement Working Group until DoD obtains approval of the standardized forms.

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments. The Deputy to the Under Secretary of Defense for Policy for Policy Support concurred with the recommendation and stated that standardized SAP formats are included in the January 1998 NISPOM Supplement Overprint. He further commented that his office would initiate action to obtain official approval of the standardized forms for use within the SAP community.

2. Develop a protective marking for sensitive unclassified information that requires restrictive distribution to the DoD special access community. Develop guidance to cover the appropriate use of the protective marking and control and accountability requirements for documents containing the protective marking, and include those requirements in DoD Pamphlet 5200.1-PH, "A Guide to Marking Classified Documents," April 1997.

Finding B. Administrative Standardization Among DoD Special Access Programs

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments. Deputy to the Under Secretary of Defense for Policy for Policy Support concurred with the recommendation and stated that the NISPOM Supplement Overprint addresses the protective marking “Handle Via Special Access Channels Only”; however, including guidance on the marking in DoD Pamphlet 5200.1-PH, “A Guide to Marking Classified Documents,” April 1997, was not possible because it was in the final stages of publication. According to the Deputy to the Under Secretary of Defense for Policy for Policy Support, the proponent of the pamphlet stated that an amendment to the publication probably would not occur until the Director, Central Intelligence, revises Directive 1/7, “Security Controls on the Dissemination of Intelligence Information.”

Part II - Additional Information

~~FOR OFFICIAL USE ONLY~~

Appendix A. Audit Process

Scope

Work Performed. We reviewed security functions at 22 SAP program offices and 22 contractor facilities. As a result of the work performed, we identified problems concerning implementation of the NISPOM Supplement and standardization of administrative documentation and protective markings. We reviewed security-related documents from June 1985 through July 1997, and PARs from January 1995 through February 1997. In addition, we included tests of management controls considered necessary.

Limitation to Audit. We primarily limited our review of DoD SAPs to those managed by the Military Departments because of milestones and resource restraints. However, DoD SAP senior managers stated that problems identified concerning implementation of the NISPOM Supplement and standardization of administrative documents and protective markings were also applicable to the Defense agencies.

Methodology

Audit Methodology. To evaluate SAP security policies, procedures and practices, we:

- ◆ reviewed and analyzed documents relating to program security and implementation of the NISPOM Supplement at each Military Department central coordinating office, program office, and contractor facility;
- ◆ developed, issued, and analyzed security questionnaires provided to the program offices and contractors;
- ◆ reviewed the SAP security eligibility process at each Military Department SAP central coordinating office, program office, and contractor facility;
- ◆ reviewed and analyzed program security guides and security classification guides;
- ◆ evaluated the effectiveness of program-specific security enhancements; and
- ◆ attended Contractor SAP/Special Access Required Security Working Group meetings.

Computer-Processed Data. We used computer-processed data from the Army Billet Structure Management System, the Navy Security Management System, and the Air Force SAP program office access rosters. We did not test the reliability of the computer-processed data; however, the reliability of the data used did not affect the audit results.

Contacts During the Audit. We visited or contacted individuals or organizations within DoD and within 22 contractor facilities. Further details are available upon request.

Audit Period, Standards, and Locations. We performed this economy and efficiency audit from October 1996 through September 1997. We performed the audit in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Use of Technical Assistance. The Quantitative Methods Division assisted in the selection of 16 of the 22 SAPs to evaluate access processing times at program offices and contractor facilities.

Management Control Program Review

DoD Directive 5010.38, "Management Control Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of the Management Control Program. We reviewed the adequacy of management controls over special access security and documentation at selected SAP program offices. Specifically, we reviewed the management controls that SAP program offices used for SAP eligibility determination, access approval, determination of currency of security program documents, and inspection of SAP contractor facilities. Because we did not identify a material management control weakness at the selected program offices, we did not assess management's self-evaluation.

Adequacy of Management Controls. Generally, program offices' management controls over access to SAP sensitive information were adequate as they applied to the audit objectives.

Appendix B. Summary of Prior Coverage

Inspector General, DoD

Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs," February 10, 1998. The report states that the Navy and the Air Force generally did not reciprocally acknowledge SAP security eligibility determinations adjudicated within and among their SAPs at the same protection level. The report also states that, although the Army established reciprocity within Army SAPs, Army access criteria were not reciprocal with Navy and Air Force SAP access criteria. As a result, Navy and Air Force SAPs implemented inefficient and redundant processes that were contrary to good business practices. In addition, the lack of reciprocity impeded access within DoD SAPs, potentially increased contractor overhead costs to the Government, and delayed performance on contracts. The report recommended that the Deputy to the Under Secretary of Defense for Policy for Policy Support develop standardized SAP security eligibility implementing criteria; establish policy, assign responsibilities, and develop operating procedures for a DoD centralized SAP database; develop a special access critical information update form; and establish, compartment, and train a cadre of special access adjudicators. In addition, the report recommended that Military Department central coordinating offices establish reciprocity by accepting access security eligibility determinations already made and establishing points of contact to identify those already accessed to a program.

The Office of the Under Secretary of Defense for Acquisition and Technology and the Office of the Deputy to the Under Secretary of Defense for Policy for Policy Support basically concurred with the recommendations of the report. Both offices commented that actions were currently underway to address the finding and recommendations identified in the report. The Navy concurred with the recommendations; the Army partially concurred with the recommendations, and the Air Force comments were not fully responsive.

Other Reviews

Senate Document 105-2, "Report of the Commission on Protecting and Reducing Government Secrecy," March 3, 1997. The report was the result of a congressional "investigation into all matters in any way related to legislation, Executive order, regulation, practice, or procedures relating to classified information or granting security clearances." The Commission made three recommendations on SAPs. First, the Commission recommended that the Security Policy Board implement the Joint Security Commission recommendation to establish a single set of security standards for SAPs.

Second, the Commission recommended that heads of agencies consider other factors besides damage to national security as a basis for establishing a SAP. Agency heads should consider cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release. Third, the Commission recommended that individuals holding valid clearances have the ability to move from one agency or special program to another without further investigation or adjudication, except in instances where a program has a polygraph requirement. As a result of the Commission's report, the Deputy to the Under Secretary of Defense for Policy for Policy Support is currently developing a DoD Implementer to the NISPOM Supplement. The Implementer will standardize SAP security measures within the DoD Components.

Joint Security Commission Report, "Redefining Security," February 28, 1994. The report addresses the processes used to formulate and implement security policies within DoD and the intelligence community. The report concludes that the clearance process is needlessly complex, cumbersome, and costly. In addition, the report highlighted several areas of concern with the current security philosophy and found that many of the problems within SAPs are because of obsolete security standards and inconsistent, program-specific applications. The report made various recommendations that would create a new policy structure, enhance security, and lower cost by avoiding duplication and increasing efficiency. The President issued Executive Order 12968 in response to the report. Also, the Secretary of Defense issued the NISPOM in response to the report and to Executive Order 12829.

Appendix C. Glossary of Supplemental Program Access Request Forms

Classified Program Security Questionnaire (SAP Format 22). The SAP Format 22, required by Air Force SAPs, asks questions regarding drug use and trafficking, alcohol abuse, criminal record, financial delinquency, bankruptcy, affiliation with organizations dedicated to the violent overthrow of the Government, and suspension or revocation of a security clearance. The Standard Form 86 covers the same questions asked in the SAP Format 22.

Defense Clearance and Investigations Index (DCII Files Check). The Defense Clearance and Investigations Index is the single, automated central repository, which identifies investigations that DoD investigative agencies conduct and personnel security determinations that DoD adjudicative authorities make.

Drug Questionnaire. The drug questionnaire asks questions regarding the experimentation, use, and selling of controlled substances such as marijuana, hashish, LSD, cocaine, amphetamines, barbiturates, or heroin. The Standard Form 86 covers drug history.

Foreign Relative or Associate Interview (SAP Format 20). The SAP Format 20 asks questions regarding names, relationships, addresses, and citizenship of any foreign relative or associates. The Standard Form 86 covers the same questions asked in the "Foreign Relative or Associate Interview" form.

Personal Financial History Form. The "Personal Financial History Form" asks specific questions regarding bankruptcies or petitions for bankruptcy. The Standard Form 86 covers the same questions asked in the "Personal Financial History Form."

Questionnaire for National Security Positions (Standard Form 86). Anyone requiring access to classified information completes Standard Form 86, and the information provided is the basis for conducting the personnel security investigation.

Appendix D. History of the National Industrial Security Program Operating Manual Supplement

Need for National Industrial Security Standards. In the early 1980s, various Government and industry security officials began to express concern over the increasing number of separate, conflicting, confusing, and sometimes arcane regulations that each Government department and agency prepared for the protection of the same kinds of information. During the 1980s, industry representatives began to accumulate data through surveys that provided evidence that security policies and procedural requirements generated independently by individual Government departments significantly increased costs without improving security. The surveys highlighted a growing need for a consolidated industrial security program. Difficulty arose, however, when it became clear that such a program would mean giving up long-standing, traditional, and parochial practices. By the end of the 1980s, industry provided documentation to support the need for a National Industrial Security Program, and the President directed a Government review to formally develop information on the issue.

National Security Review. On April 4, 1990, President Bush signed a National Security Review entitled, "The National Industrial Security Program," which directed a review of the Government's industrial security programs to determine the feasibility of establishing a single program applicable to all Government departments and agencies. In 1990, the review group conducted a survey of 6 Government agencies and 13 DoD agencies. A key finding of the survey was that the Government used 47 different standards, manuals, and directives to implement security measures. The documents created a significant regulatory burden to industry and Government. The Government lacked uniform personnel security requirements and reciprocity of investigations, which caused unnecessary costs from redundant investigations and lost time while personnel waited for clearances. The survey confirmed the Government's use of multiple rules to protect information of the same sensitivity and inconsistent application and enforcement of those rules.

Proposal and Establishment of the National Industrial Security Program. As a result of the review, the President directed that a task force establish a National Industrial Security Program that would develop program criteria, improve administration, establish uniform security standards and procedures applicable to all organizations, establish a centrally directed system of oversight and compliance, and establish a program to continually evaluate personnel security methods that would assist in early detection of potential espionage candidates. The report to the President, issued in September 1991, proposed an industrial security program that protects classified information with reasonable standards in response to the threat, vulnerability, and value of the asset. The proposed program allows the imposition of some supplemental standards or protection techniques required to protect information of particular sensitivity, to meet intensified threats, or to mitigate specific vulnerabilities.

Appendix D. History of the National Industrial Security Program Operating Manual Supplement

Executive Order 12829, "National Industrial Security Program," January 1993, established the National Industrial Security Program as a single, integrated, cohesive industrial security program to protect classified information and to preserve information vital to the Nation's security. The Executive order directed the Secretary of Defense, as the Executive Agent, to issue and maintain the NISPOM. The NISPOM would set forth the specific requirements, restrictions, and safeguards that Government agencies would use to protect classified information and special classes of classified information. The Executive order established a 1-year deadline for issuance of the NISPOM, and directed Government agencies to develop and issue specific guidance to implement the NISPOM 180 days after its issuance. The President amended the Executive order on December 14, 1993, to allow the Secretary of Defense to issue the NISPOM after the Joint Security Commission's report on "Redefining Security," February 1994.

The February 1994 report of the Joint Security Commission, convened at the request of the Secretary of Defense and the Director, Central Intelligence, addressed the Commission's concern with the current security philosophy and reported that problems inherent to SAPs were from obsolete security standards and inconsistent program-specific applications. The Commission recommended, among other things, a single security policy to replace the numerous existing policies that were often inconsistent and sometimes contradictory. The Commission believed that a single security policy would result in reciprocity across the security arena, with subsequent reductions in cost and improvements in efficiency.

National Guidance. DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," January 1995, is the single Government regulation outlined in Executive Order 12829, and it provides requirements for protection of classified information. The NISPOM would serve as the only manual for protection of collateral classified information, and a "baseline" for protection of special classes of classified information, including SAPs.

DoD Manual 5220.22-M-Supplement 1, "National Industrial Security Program Operating Manual Supplement," February 1995, provides both mandatory and 45 optional enhancements for the protection of information used in SAPs and SAP-type compartmented efforts. To facilitate concurrence between the DoD, the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency, the Executive Agent did not provide instructions on how to select options for SAPs or how to "implement" the supplement. During the development of the NISPOM Supplement, the NISPOM Supplement Working Group established 26 "SAP Formats," which provided standardized administrative forms for use in SAPs. However, to ensure concurrence between the Federal agencies listed above, the Executive Agent did not include the SAP Formats in the final version of the NISPOM Supplement.

Appendix E. Text Differences Relating to Secret Accountability and Engineering Notebooks

NISPOM and NISPOM Supplement	Joint Implementor Navy	Joint Implementor Air Force
<p>NISPOM 5-201. The document accountability system for Secret material is eliminated as a security protection measure, The U.S. Government reserves the right to retrieve its classified material.... The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in a reasonable period of time.</p> <p>NISPOM 5-205 b. Classified working papers, such as notes and rough drafts generated by the contractor in the preparation of a finished document, shall be: (1) dated when created; (2) marked with its overall classification and with the annotation "WORKING PAPERS," and (3) destroyed when no longer needed.</p>	<p>5-201.2.a. A matrix requires Receipt and Dispatch Control for waived, unacknowledged, and acknowledged programs classified as Secret Codeword. For waived programs, the matrix also requires Personal Signature Control and Annual Inventory.</p> <p>5-205.b(2). All Top Secret and Secret working papers shall be properly classified and program-marked with a SAP cover sheet listing the date of origin and including the annotation WORKING PAPERS. Top Secret working papers and accountable Secret working papers (see matrix in 5-201) shall be controlled or destroyed within 90 calendar days from their date of origin.</p>	<p>5-201.1.d. Secret/Special Access Required accountability will be at the command level. Therefore, the Government agency or contractor will maintain a system that accounts for Secret Special Access Required material when the contractor receives or dispatches it</p> <p>5-205 b(1). Formally account for classified, mission-revealing working papers and draft materials no later than 90 days from the date of origin. Afford physical protection to those documents equivalent to accountable documents at all times. Bring Top Secret working papers under accountability by the end of the workday.</p>

Appendix E. Text Differences Relating to Secret Accountability and Engineering Notebooks

NISPOM and NISPOM Supplement	Joint Implementor Navy	Joint Implementor Air Force
<p>NISPOM 4-202. All classified material shall be marked . on the face of all classified documents</p> <p>NISPOM Supplement 4-202. An engineer's notebook is a working record of continually changing program technical data... The outer cover and the first page will be marked with the highest classification level contained in the notebook.... Other requirements pertaining to the notebooks may be imposed by the PSO [program security officer].</p> <p>NISPOM 4-214. Unless a requirement exists to retain material...for a special purpose, there is no need to mark, stamp, or otherwise indicate that the material is classified. (NOTE Such material developed in connection with the handling, processing, production, and use of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and its destruction at the earliest practical time.)</p>	<p>4-214. Working papers shall be so identified and marked with the proper classification. (See paragraph 5-205.b. for additional Information related to working papers.)</p>	<p>4-214. Working papers shall be so identified and marked with the proper classification. (See paragraph 5-205.b. for additional information related to working papers.)</p>

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Deputy Under Secretary of Defense (Acquisition Reform)
Deputy Under Secretary of Defense (Industrial Affairs and Installations)
Director, Special Programs
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense for Policy
Deputy to the Under Secretary of Defense for Policy for Policy Support
Director for Special Programs
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Director for Special Programs
General Counsel, Department of Defense
Assistant to the Secretary of Defense (Public Affairs)
Director, Special Access Program Coordination Office

Joint Staff

Director, Joint Staff
Deputy Director for Operations (Current Operations)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief, Technology Management Office, Army Staff

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Assistant Secretary of the Navy (Research, Development, and Acquisition)
Auditor General, Department of the Navy
Director, Special Programs Division, Chief of Naval Operations
Director, Oversight Division, Inspector General for the Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Acquisition)
Director, Special Programs
Security Director

Department of the Air Force (cont'd)

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Director, Security and Special Programs Oversight

Other Defense Organizations

Director, Defense Advanced Research Projects Agency
Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Commander, Defense Contractor Management Command
Director, National Reconnaissance Office
Director, National Security Agency
Inspector General, National Security Agency
Director, Defense Security Service
Inspector General, National Imagery and Mapping 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
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal
Justice, Committee on Government Reform and Oversight
House Committee on National Security
House Permanent Select Committee on Intelligence

Part III - Management Comments

~~FOR OFFICIAL USE ONLY~~

Under Secretary of Defense for Acquisition and Technology Comments



ACQUISITION AND
TECHNOLOGY

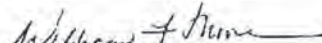
FOUO
OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

7 JAN 1998

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE (ATTN: (b)(6), PROJECT MANAGER)

SUBJECT **Audit Report on Special Access Program Security Issues (Project No. 7AD-0005.01, 12 November 1997)**

I have reviewed the draft report of the "Special Access Program Security Issues" and appreciate the work you and your team have done in accomplishing this audit. My comments on this report are in the attachment.


William F. Moore
Major General, USAF
Director, Special Programs

Attachment

cc
DUSD(AR)
DUSD(IA&I)

FOUO 

FOUO

OUSDA(A&T)/DSP Comments on DoD IG Audit Report, "Access Reciprocity Between DoD Special Access Programs (Project No. 7AD-0005.00)"

- 1 I have the following general observations about the report
 - a Page 2, "Special Access Programs". The bullets under this paragraph discuss the criteria for establishing a SAP and they are paraphrased from DoD 5200 1-R (8-100, page 8-1) A better description of the criteria for establishing a SAP can be found in DoD Directive O-5205.7, page 2

Added

"Any DoD program or activity [employing] enhanced security measures exceeding those normally required by DoD 5200 1-R for information at the same classification level shall be established, approved and managed as a DoD SAP. Examples of such enhanced security measures include the following: use of any special terminology, including code words, other than an unclassified nickname, to identify or control information dissemination, personnel security investigative or adjudicative requirements more stringent than those required for a comparable level of classified information, specialized non-disclosure agreements, exclusion of a classified contract, [or] a centralized billet system to control the number of personnel authorized access "

- b Page 20, "Program Access Requirements and Documents"

- (1) We are actively working to establish common "levels" of SAP adjudication into which all DoD SAPs can be categorized. When this is combined with a DoD training program for all SAP adjudicators, it will facilitate reciprocity among SAPs. I agree that what is needed is a common set of standards for adjudication to be consistently applied to all DoD SAPs within each defined "level". I would envision using our current cadre to provide matrix support to the SAP Coordination Office. I would ensure common standards and training for all the SAP adjudicators. A matrix organization would implement the appropriate level of adjudication required for each individual and the appropriate adjudication information would be entered into a standard database system. We will conduct a comprehensive study of how to best accomplish this. Currently, we believe this can be accomplished by adding a field to the existing DCII database. This would make adjudication information available to the program PSOs and they would revalidate the currency of the individual's security clearance and investigation information, as required.

Page 19

- (2) What is currently done by the PSOs is not actually a readjudication, but rather it is a revalidation of the individual's suitability for access. Much of the need for this revalidation will be mitigated when we establish the common adjudicative standards and training process outlined above in 1 b (1). However, there will always be the need to ensure the currency of the

FOUO

FOUO

clearance and investigation information for any individual seeking SAP access. We must ensure that new information does not adversely impact an individual's suitability for access. I call this process a revalidation rather than a readjudication.

- c. Page 22, "Time Factor" I agree, there is a need to ensure that SAP accesses are processed in a timely fashion. You state that the time taken to readjudicate PAR packages for multiple SAP accesses is excessive and costly. As I discussed above in 1 b (2), PSO are currently revalidating rather than readjudicating PAR packages. By establishing common SAP levels of adjudication and entering the resulting adjudication information into a common database, we will reduce both the time and cost involved with the current process of gaining access to multiple SAPs.
2. The SAPCO basically concurs with the focus and recommendations of this report. Action is already well underway to address most of your findings.

FOUO

Deputy to the Under Secretary of Defense for Policy for Policy Support Comments



POLICY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000



12 JAN 1998

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: (b)(6), PROJECT MANAGER)

SUBJECT: Audit Report on Special Access Program Security Issues
(Project No 7AD-0005 01)

Reference is made to the subject draft report, dated 12 November 1997

We appreciate the audit team's hard work on the subject audit. We concur in the recommendations and have provided our comments on them in the attachment. As explained in the attachment, the DoD NISPOMSUP Overprint is in its final stages of preparation and is expected to be approved in January 1998. Selected portions of the overprint respond directly to several of the recommendations contained in your audit report.

Linton Wells II
Deputy to the USD(P)
for Policy Support

Attachment
As stated



DoD IG Report - Project No. 7AD-0005-01 (12 Nov 97)

COMMENTS ON THE REPORT'S RECOMMENDATIONS

Recommendation A.1.a.: Finalize and issue the DoD NISPOMSUP Implementer

The DoD NISPOMSUP Overprint is in its final stages of publication and is expected to be forwarded in January 1998 to the Deputy Secretary of Defense for approval. The document was developed and coordinated by the Security Policy Board's Special Access Program Security Standards Working Group. It contains uniform security guidance for all DoD SAPs to facilitate reciprocity as mandated in Recommendation Two of the Report of the Commission on Protecting and Reducing Government Secrecy. The Overprint is being published in an automated format in consonance with guidance contained in the DoD Defense Reform Initiative. Implementation of the Overprint will greatly enhance standardization and reciprocity within the DoD SAP community.

Recommendation A.1.b.: Provide contractor guidance on non-accountable classified documents and control and accountability of engineering notebooks

In the Overprint, the approach to providing contractor guidance on retrieval and disposition of non-accountable documents is based primarily on the type of information concerned, as opposed strictly to the level of security classification. Specifically, Appendix G (Security Documentation Retention) to the Overprint contains a matrix which displays types of classified or unclassified information involved (e.g., visits, waivers, alarm-test records, and recurring reports), the retention entity, and disposition/destruction guidance. This matrix should provide invaluable guidance on the matter. Regarding engineering notebooks, paragraph 5-206 gives detailed guidance on the accountability, marking, reproduction, and retention of working notebooks (e.g., engineering notebooks).

Recommendation A.2.: Develop policy to formally implement the Single Process Initiative within DoD SAPs.

In our article in DoD Industrial Security Letter 97-1 (July 1997), contractors were encouraged to identify opportunities for implementing the Single Process Initiative (SPI) within DoD SAPs. Where appropriate, we further intend to work with the appropriate entities to explore ways to better regularize procedures for SPI implementation within DoD SAPs.

Recommendation B.1. Review/standardize SAP formats and forms and obtain DoD approval of SAP forms.

Agreed SAP formats are included in the Overprint for use by the OSD-level and Component-level SAP Central Offices. Action will commence shortly to obtain official approval of standardized forms for use within the SAP community.

Recommendation B.2. Develop procedures on protective marking for sensitive unclassified material which must remain in SAP channels.

Paragraph 4-204 and Appendix A (Definitions) of the Overprint address the protective marking "Handle Via Special Access Channels Only" for use, inter alia, on unclassified material which must remain in SAP-controlled channels. It was not feasible to include this guidance in the newly-published DoD Pamphlet 5200.1-PH (April 1997) because it was already in its final stages of publication. The proponent agency's representative advised that an amendment to the publication would not likely occur until after publication of a revised Director of Central Intelligence Directive No. 1/7 (Security Controls on the Dissemination of Intelligence Information).

Department of the Army Comments

Final Report
Reference



REPLY TO
ATTENTION OF

DACS-DMP

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
200 ARMY PENTAGON
WASHINGTON DC 20310-0200

6 January 1998

MEMORANDUM FOR INSPECTOR GENERAL, DOD, ATTN: (b)(6)

SUBJECT: Draft of Audit of Special Access Program Security Issues (Project No 7AD-0005.01)

1 Army submits the following comments on the subject report:

a. Recommendation A.3.: We recommend that the Chief, TMO, revise AR 380-381, specifically to correlate Army Special Access Program Categories I, II, and III, with DoD special access program categories for acknowledged, unacknowledged, and waived to reflect consistency with DoD Instruction 5205.11. Because Army Regulation 380-381 is ready for publication, the Army can use a change notification to make the revision.

b. *NONCONCUR* We suggest that you revise recommendation A.3. to read: We recommend that TMO publish guidance to Army Special Access Programs categorizing SAPs as waived, unacknowledged, or acknowledged so that the programs can interpret guidance from DoD.

c. *RATIONALE:* Army uses SAP categories I, II, and III to specify security measures that are distinct from decisions to waive or not waive and acknowledge or not acknowledge a SAP (See figure 3-1, AR 380-381) Army categories I, II, and III do not result in conflicting or inconsistent guidance to DoD contractors. The DoD SAP Security Working Group has not finalized the correlation between DoD SAP categories, the number of SAP sensitivity levels, and security enhancements available to each sensitivity level. Additionally, revising an Army Regulation is not the most effective method to implement evolving guidance. TMO will publish guidance to all Army SAPs which will designate the appropriate DoD category for each Army SAP. Evidence of Army compliance with the use of DoD categories is the annual SAP report. Army identifies SAPs by DoD category in this report.

2 Additional comments

a. Page 8, first paragraph Recommend that you delete this paragraph

RATIONALE. The original intent of the DoD SAP typology was for each to correspond to a sensitivity level and applicable security enhancements. The sensitivity levels and applicable enhancements are still under development. DoD guidance did not direct Army to revise AR 380-381

Printed on Recycled Paper

Revised

Page 7

DACS-DMP

SUBJECT Draft of Audit of Special Access Program Security Issues (Project No 7AD-0005.01)

b Page 19., last sentence. Recommend that you revise this sentence to read "To maintain access eligibility, SAP accessed personnel must have periodic reinvestigations every 5 years" Also, delete the next sentence in that paragraph.

Page 27

RATIONALE The purpose of the PR is to maintain access eligibility, not establish reciprocity Access determinations are based on a "need-to-know" decision after access eligibility has been verified

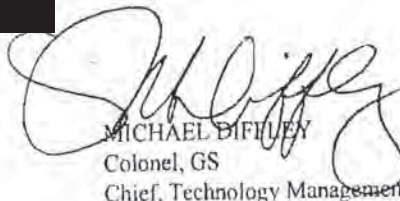
c Page 22 , "Time Factor" paragraph Delete references to Army in this paragraph. Page 23 , Table 3 Revise

Page 20
Page 21

RATIONALE. Regardless of whether access eligibility determinations are reciprocally acknowledged, a contractor employee will be required to submit some form of access request document upon which to base the "need-to-know" determination This will be required for access to each program. The table is misleading because some form of access request document will always be required for each program The duplication is in the number and types of supporting documentation included in the PAR

3 Army concurs with the conclusion that standard DoD access request forms and reciprocally acknowledged access eligibility determinations will reduce the administrative burdens currently imposed on contractors

4 TMO POC is (b)(6)



MICHAEL D'ALMEIDA
Colonel, GS
Chief, Technology Management Office

Department of the Air Force Comments



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

OFFICE OF THE SECRETARY

MEMORANDUM FOR: DOD IG (b)(6)

JAN 12 1998

SUBJECT: Air Force Response to DoD IG Audit, "Special Access Program Security Issue"

FROM: SAF/AAZ

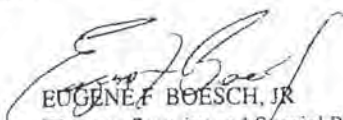
After review of subject audit the Air Force provides the following comments:

FINDING A: Concur with comment. The Air Force co-authored the proposed DoD NISPOM Supplement overprint and intends to follow the guidance the overprint proscribes. The draft DoD NISPOM Supplement Overprint is derived directly, and nearly verbatim, from the Air Force/Navy Implementor, and subsequent Navy and Air Force Program Security Directives. As such, the Air Force has been using the NISPOM Supplement list of options since the supplement's inception. In the rush towards standardization the audit prescribes minute administrative efficiencies to the detriment of overall program security and subsequent program management efficiencies. The audit correctly notes that the Air Force allows each Program Security Officer to tailor security (through the selection of NISPOM Supplement options) to their specific program based first, and foremost, on the security risk. Contrary to the audit's findings, the USAF firmly supports the concept that security is the paramount issue in developing and executing a special access program—not relieving involved government and contractor agencies of minor administrative chores. Security efficiency is gained through the implementation of NISPOM Supplement options tailored to the threat to a specific program, not through the implementation of options to a class of programs facing different threats.

FINDING B: Concur with comment. The forms used in the proposed DoD NISPOM Supplement were drafted by the USAF and predominantly derived from the Air Force-Navy Implementor and the Air Force Program Security Directive. Every USAF SAP followed the HQ USAF guidance provided issued in the Air Force-Navy Implementor and subsequent Air Force Program Security Directive—including the forms that are now found in the DoD Overprint. Contrary to the audit's findings, the Air Force implemented the NISPOM Supplement consistently **within** USAF SAP's, but not **across** a class of USAF SAP's (Level 1, 2, or 3), which is what the audit actually reveals. The differentiation is crucial, as stated previously, each USAF SAP Security Officer tailors security to their program based on threat and within the confines of the NISPOM Supplement (or is granted a waiver). Each USAF SAP, including the Program Security Directive, receives DepSecDef approval and subsequent Congressional notification. Each SAP is unique, not only in its purpose, but the threat it faces. This audit report does

not provide any conclusive evidence that there are efficiencies to be gained by categorizing, and assigning NISPOM Supplement options, to SAP's by class—the security efficiencies are obtained through tailoring security to the threat faced by a specific program and using only the options necessary to provide the applicable level of security. Further research would have demonstrated that the proposed DoD Overprint provides the flexibility to SAP Security Officers to use only the options necessary for the adequate protection of their program. The concept is validated by the heavy reliance on the Air Force-Navy Implementor and Air Force and Navy Program Security Directives that is found in the proposed DoD Overprint. Additionally, this concept will continue to be executed within USAF SAP's and continue to reflect full adherence to the NISPOM Supplement and DoD Overprint.

POC is (b)(6)


EUGENE F. BOESCH, JR.
Director, Security and Special Program
Oversight

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

(b)(6)



~~FOR OFFICIAL USE ONLY~~