April 19, 2006

Human Capital

DoD Security Clearance Process at Requesting Activities
(D-2006-077)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

DES-DE	Defense Logistics Agency Enterprise Support Europe
DSS	Defense Security Service
EPSQ	Electronic Personnel Security Questionnaire
e-QIP	Electronic Questionnaire for Investigations Processing
GAO	Government Accountability Office
IG	Inspector General
JPAS	Joint Personnel Adjudication System
NAC	National Agency Check
OPM	Office of Personnel Management
PSI	Personnel Security Investigation
USD(I)	Under Secretary of Defense for Intelligence

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

April 19, 2006

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
NAVAL INSPECTOR GENERAL
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Report on DoD Personnel Security Clearance Process at Requesting Activities (Report No. D-2006-077)

We are providing this report for review and comment. We considered management comments when preparing the final report. The Under Secretary of Defense for Intelligence comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Department of the Army, Department of the Navy, and Defense Information Systems Agency comments were partially responsive. The Department of the Air Force did not provide comments on Recommendation 3. The Defense Logistics Agency comments were nonresponsive. We request additional comments from all on Recommendation 3. by May 19, 2006.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudCM@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kimberley A. Caprio at (703) 604-9202 (DSN 664-9202) or Mr. Riccardo R. Buglisi at (703) 604-9314 (DSN 664-9314). For the report distribution, see Appendix D. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Richard B. Jolliffe

Richard B. Jolliffe
Assistant Inspector General
Acquisition and Contract Management

Department of Defense Office of Inspector General

Report No. D-2006-077 **April 19, 2006**
(Project No. D2005-D000CB-0136.000)

DoD Personnel Security Clearance Process at Requesting Activities

Executive Summary

Who Should Read This Report and Why? Officials in the Office of the Under Secretary of Defense for Intelligence and the Defense Security Service, and management and personnel in the Services and Defense agencies responsible for security clearances and personnel security investigations should read this report. The report discusses impediments to the DoD security clearance process and the need to develop and issue policy to ensure consistent implementation of the personnel security clearance program.

Background. This report discusses the DoD personnel security clearance process at requesting activities. Security clearances and personnel security investigations are key elements in protecting national security by determining whether a person is eligible under DoD policy for access to classified information, including top secret, secret, and confidential. In January 2005, the Government Accountability Office identified long-standing delays in completing investigations, a growing backlog, and no effective method to estimate total workload requirements within DoD. Such problems with timeliness and quality in the personnel security clearance process can affect our national security.

Results. All 26 DoD military and civilian requesting activities we visited experienced difficulties in effectively and efficiently processing personnel security investigation requests for military and civilian personnel. Specifically, requesting activities were unable to rely on the Joint Personnel Adjudication System for accurate and complete personnel data, experienced increased workloads, and received rejected personnel security investigation requests from the Office of Personnel Management. Additionally, security personnel were not always knowledgeable in the personnel security process and systems used. Finally, the DoD controls over the management of the DoD Personnel Security Clearance Program were not sufficient to ensure that the requesting activities could efficiently and effectively process DoD personnel security clearance requests. As a result, requesting activities may continue to experience delays in the security clearance process, which may impact national security, completion of critical DoD missions, and support of the warfighter. The Office of the Under Secretary of Defense for Intelligence should update DoD policy for the security clearance program, establish guidelines for publishing the policy, and coordinate with the Services and Defense agencies to improve communication with requesting activities and expedite resolution of identified issues. In addition, the Services, Defense Information Systems Agency and Defense Logistics Agency should update their respective policies for the personnel security clearance program in accordance with DoD policy. (See the Finding section for detailed recommendations.)

Management Comments and Audit Response. The Under Secretary of Defense for Intelligence, Acting Director of Security concurred, stating that the organization is working on drafting an update to DoD Regulation 5200.2-R and expect to have a draft ready for staffing and coordination by July 2006, with publication anticipated by summer 2007. The Acting Director also stated that the organization is exploring options to best communicate with DoD Components on changes to the security clearance process and future plans, and to solicit input from field activities. The Army Director, Counterintelligence, Human Intelligence, Disclosure and Security Directorate, Office of the Deputy Chief of Staff, G-2 partially concurred with the recommendation to update Army policy, stating that complete security clearance information is available via Army memoranda and other communication. While issuing memorandums supplements Army Regulation 380-67, the Regulation should be updated to include current information on program management and investigative responsibilities, security clearance systems, training requirements, and submission processes, types, and scopes of personnel security investigations. The Chief of Naval Operations, Special Assistant for Naval Investigations and Security partially concurred with the recommendation, stating that a Navy personnel security program policy is due for signature in May 2006, and that the Navy Security Web site contains additional information on the security clearance process. While these actions met the intent of the recommendation, the Secretary of the Navy Instruction 5510.30A did not provide information on the contents of the Navy Personnel Security Program Policy Regulation, which should include updated or complete information on investigative responsibilities, security clearance systems, training requirements, or submission processes, types and scopes of personnel security investigations. The Air Force Director of Security Forces, Information Security did not comment on the recommendations, but maintained that Air Force Instruction 31-501 contains information on the personnel security clearance program, but lacked training requirements. However, the Air Force Instruction lacked complete information on the types and scopes of personnel security investigations.

The Defense Information Systems Agency Director, Manpower, Personnel and Security generally concurred with the recommendation, noting that the Security Division is revising the Defense Information Systems Agency Instruction 240-110-8, which is estimated for completion in May 2006, and that information on the personnel security clearance process is included in the Defense Information Systems Agency Personnel Security Standard Operating Procedures. However, the standard operating procedures and training requirements should be included or referred to in the updated Defense Information Systems Agency Instruction 240-110-8. The Director, Defense Logistics Agency Enterprise Support partially concurred with the recommendation and stated that the Defense Logistics Agency One Book or Personnel Security Program Guidebook provides information on the critical elements of the personnel security clearance process, and that despite lack of written training requirements, personnel security specialists are trained at least every 2 years. However, the policy did not include complete information on the types and scopes of personnel security investigations. Additionally, while the Defense Logistics Agency internal training meets the intent of the recommendation, the Defense Logistics Agency policy should include training requirements.

We request that the Army Deputy Chief of Staff for Intelligence; Director, Naval Criminal Investigative Service; Air Force Director of Security Forces, Information Security; Defense Information Systems Agency Director, Manpower, Personnel and Security; and Director, Defense Logistics Agency provide comments on the final report by May 19, 2006. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Finding

Appendixes

Management Comments

Background

Personnel Security High Risk Area. For over a decade, Government Accountability Office (GAO) reports have documented persistent problems in the DoD security clearance process. In January 2005, GAO designated the DoD Personnel Security Clearance Program as a high-risk area due to long-standing delays in completing investigations, a growing backlog, no effective method to estimate total workload requirements, and because DoD has approximately two million active security clearances. Such problems with timeliness and quality in the personnel security clearance process can affect our national security. Specifically, delays in completing clearances can result in negative consequences such as nonproductive time while awaiting clearances and the loss of highly qualified candidates. Delays in renewals of clearances for persons already doing classified work can lead to a heightened risk of disclosure of classified information. In the FY 2005 "Annual Statement Required Under the Federal Managers Financial Integrity Act of 1982," DoD reported 329,000 pending security clearance investigations for DoD military, civilians, and contractors.[1]

Security Clearances and Personnel Security Investigations. Security clearances and personnel security investigations (PSI) are key elements in protecting national security. A security clearance is a determination that a person is eligible under DoD policy for access to classified information. Clearances allow personnel to access classified information categorized into three levels: top secret, secret, and confidential. The damage to national defense and foreign relations that unauthorized disclosure could reasonably be expected to cause ranges from "exceptionally grave damage" for top secret information to "damage" for confidential information. A PSI is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he or she is eligible to access classified information or for an appointment to a sensitive position or position of trust. DoD uses PSIs to determine an individual's eligibility for a security clearance. The types of PSIs vary based on the level of security clearance necessary for a given sensitive position. DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, outlines criteria for sensitive positions and the corresponding clearance levels. Each clearance level requires a different type of PSI. For additional information, see Appendix C.

DoD Policy. DoD Directive 5200.2, "DoD Personnel Security Program," April 1999, establishes policy to ensure that military, civilian, and contractor personnel assigned to and retained in sensitive positions are and remain reliable, trustworthy, and loyal to the United States. Additionally, DoD Regulation 5200.2-R establishes DoD personnel security policies and procedures; prescribes the types and scopes of PSIs; and provides criteria, standards, and guidelines upon which DoD should base personnel security determinations. The Directive assigns oversight responsibility for the DoD Security Clearance Program for military, civilian, and contractor employees to the Under Secretary of

[1] Our audit addressed only the security clearance process at requesting activities for DoD civilian and military personnel. We did not review the security clearance process for contractors.

Defense for Intelligence (USD[I]).[2] Within USD(I), the Deputy Under Secretary of Defense for Counterintelligence and Security is responsible for the DoD Personnel Security Clearance Program. In addition to the DoD-level policy, the Services and Defense agencies also developed policies for the Personnel Security Clearance Program.[3] We reviewed policies for the Army, Navy, Air Force, Defense Information Systems Agency and Defense Logistics Agency.

Intelligence Reform and Terrorism Prevention Act of FY 2004. In July 2004, the National Commission on Terrorist Attacks Upon the United States released a comprehensive report chronicling the circumstances leading up to the terrorist attacks of September 11, 2001. The report identified that the security clearance process could not satisfy the demand for personnel security clearances within the Federal Government or private sector. As a result, Section 3001 of the Intelligence Reform and Terrorism Prevention Act of FY 2004 (Intel Reform Act) reformed the personnel security clearance process. The Intel Reform Act describes reducing the length of the security clearance process and setting goals for the process. The Intel Reform Act states that by December 2006, investigative agencies should complete at least 80 percent of the PSIs within 120 days, allowing 90 days for investigation and 30 days for an eligibility determination. The Intel Reform Act decreases these timelines in December 2009, when investigative agencies and central adjudication facilities must complete at least 90 percent of PSIs within 40 and 20 days, respectively.

Key Agencies in the Security Clearance Process. In addition to USD(I), three key agencies are involved in the DoD security clearance process: the Office of Management and Budget, the Defense Security Service (DSS), and the Office of Personnel Management (OPM). In response to the Intel Reform Act, the President designated the Office of Management and Budget to be responsible for the security clearance process. DSS, under the direction, authority and control of USD(I), offers comprehensive security education and training to DoD and other Government entities, and is also responsible for managing the Joint Personnel Adjudication System (JPAS). OPM conducts PSIs for DoD civilian and military personnel requiring initial or continued access to classified material, and for individuals in positions of trust.

Service and Defense Agency Level Responsibilities. Each Service has designated offices responsible for the personnel security clearance program. For the Army, the Deputy Chief of Staff for Intelligence (Army G-2) is responsible for formulating policy that governs Army personnel security and submitting PSI requests. The Navy designated the Director, Naval Criminal Investigative Service as the responsible party for establishing, directing, and overseeing the Navy

[2] The Defense Authorization Act for FY 2003 established USD(I) in May 2003 to organize all intelligence and intelligence-related oversight and policy guidance functions within the Office of the Secretary of Defense. Prior to May 2003, DoD assigned duties associated with the DoD Security Clearance Program to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.

[3] Army Regulation 380-67, "Personnel Security Program," dated September 9, 1988; Navy Instruction 5510.30A, "Department of the Navy Personnel Security Program," dated March 10, 1999; Air Force Instruction 31-501, "Personnel Security Program Management," dated January 27, 2005; Air Force Policy Directive 31-5, "Personnel Security Program Policy," dated August 1, 1995; Defense Information Systems Agency Instruction 240-110-36, dated November 22, 2002; and Defense Logistics Agency Directive 5025.30, dated March 18, 2005.

personnel security clearance program. The Chief, Information Security Division, Air Force Chief of Security Forces is responsible for developing Air Force personnel security policy. In addition, Defense agencies we visited assigned responsibilities for the personnel security clearance program. The Defense Finance and Accounting Service assigned responsibility for the personnel security clearance program to the Director, Human Resources. The Defense Information Systems Agency assigned the Manpower Personnel, and Security Directorate Chief, Security Division to be responsible for personnel security clearance program, and the Defense Logistics Agency assigned the Staff Director, Defense Logistics Agency Enterprise Support, Public Safety Office.

Transfer of Investigative Function. On February 20, 2005, DoD transferred the PSI function from DSS to OPM to improve the timeliness of PSIs and allow DoD to concentrate its efforts on other security functions that are part of the Department's core mission responsibilities. According to DoD officials involved in the transfer, DoD represents approximately 80 percent of the investigative workload for OPM. The Memorandum of Agreement transferring the PSI function to OPM requires DoD and OPM to work with the Office of Management and Budget to develop a Joint Improvement Plan specifically addressing timeliness of the overall security clearance process.

After the transfer, DSS established the DSS Clearance Liaison Office to support USD(I) with oversight, planning, developing, and communicating DoD policies regarding the DoD Personnel Security Program. The DSS Clearance Liaison Office is an intermediary for DoD, DoD Components (including industry and central adjudication facilities), and OPM for security clearance issues. The DSS Clearance Liaison Office also assists and supports planning, procedures, studies, and policies in USD(I). The DSS Clearance Liaison Office focuses on systemic issues, serves as the DoD facilitator to OPM, and helps OPM prioritize DoD PSIs. The Clearance Liaison Office consists of seven employees functionally aligned with the Services, Defense agencies, and industry.

Objectives

The overall objective was to determine whether the DoD personnel security clearance program was effectively and efficiently managed at the requesting activity level. Specifically, we evaluated the processes for determining security clearance requirements, initiating and updating security clearances, and monitoring the accuracy and completeness of personnel security questionnaires. We also evaluated the management control program as it relates to the overall objective. See Appendix A for a discussion of the scope and methodology and Appendix B for prior coverage related to the objectives.

Managers' Internal Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We reviewed the adequacy of DoD management controls over the DoD Personnel Security Clearance Program. We also reviewed the adequacy of management's self-evaluation of those controls.

Adequacy of Management Controls. We identified material management control weaknesses for DoD as defined by DoD Regulation 5200.2-R. DoD controls over the management of the DoD Personnel Security Clearance Program were not sufficient to ensure that the requesting activities could efficiently and effectively process DoD personnel security clearance requests. If management implements all recommendations, DoD may increase their ability to process security clearance requests in a timely manner. A copy of the report will be provided to the senior officials in charge of management controls for the DoD Personnel Security Clearance Program.

Adequacy of Management's Self-Evaluation. In FY 2003, USD(I) identified the personnel security investigations program as a systemic weakness within the Office of the Secretary of Defense because PSIs did not meet standard timeliness goals. DoD has made significant management and other changes to remedy this problem. The FY 2005 "Annual Statement Required Under the Federal Managers Financial Integrity Act of 1982" states that USD(I) will accurately track the number of investigations, cost, and other data for workload projections through improvements in JPAS. Additionally, USD(I) established timelines to determine performance results. USD(I) set the target corrective date of fourth quarter FY 2006.

Effectiveness and Efficiency of the Security Clearance Process at DoD Requesting Activities

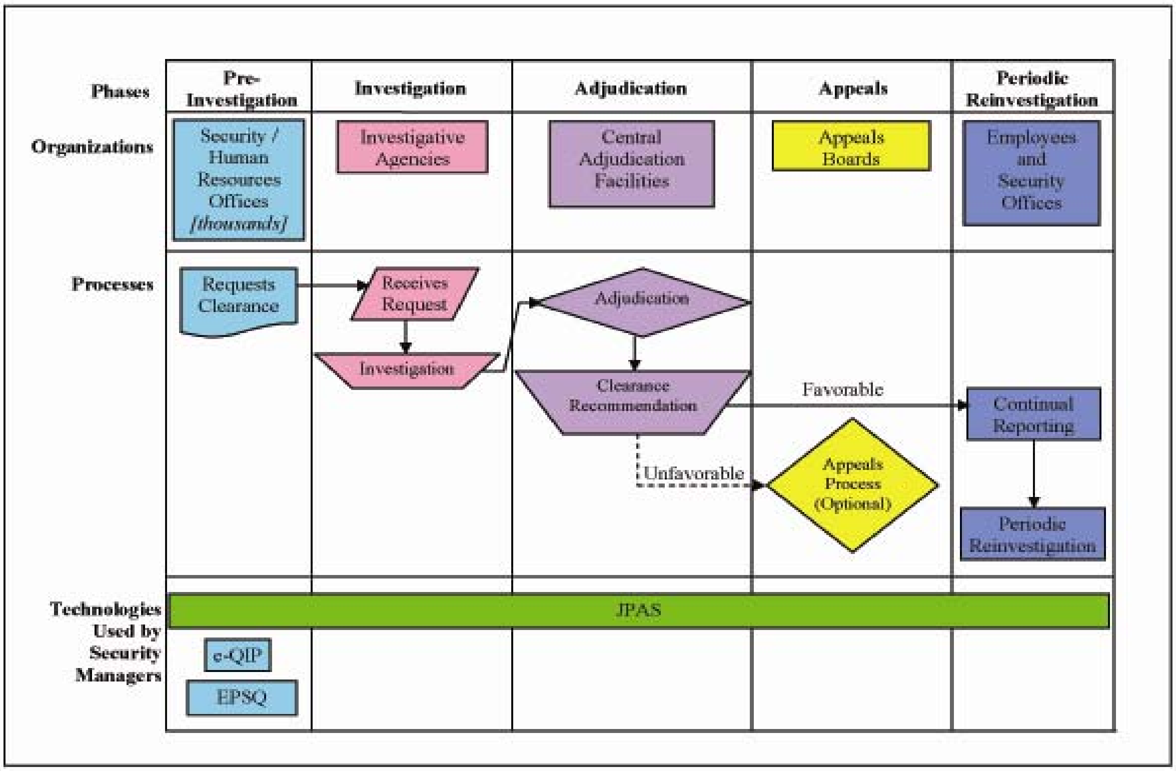
All 26 DoD military and civilian requesting activities we visited experienced difficulties in effectively and efficiently processing PSI requests for military and civilian personnel. This occurred because USD(I) did not:

- establish training requirements for security managers, or
- perform adequate management or oversight as required by DoD Regulation 5200.2-R.

In addition, USD(I), the Services, and Defense agencies we visited did not consistently update policy to include complete information on eight key elements. As a result, requesting activities may continue to experience delays in the security clearance process, which could impact the completion of critical DoD missions.

Security Clearance Process

Process for Requesting Security Clearances. Although the process for requesting a security clearance differs slightly among DoD Components, the security clearance process has five phases: Pre-Investigation, Investigation, Adjudication, Appeals, and Reinvestigation. In the Pre-Investigation phase, requesting activities determine requirements for access to classified information and submit PSI requests via the Electronic Questionnaire for Investigations Processing (e-QIP) or the Electronic Personnel Security Questionnaire (EPSQ) to OPM. During the Investigation Phase, the investigative agency performs PSIs by conducting subject interviews and background investigations. In the Adjudication Phase, the central adjudication facility reviews the results from the Investigation Phase and recommends whether the individual is eligible for access to classified information. The Appeals Phase gives individuals the option to appeal an unfavorable recommendation from the central adjudication facility. Finally, in the Reinvestigation Phase, security managers maintain security records and track investigation dates for reinvestigation using JPAS. The figure on the following page depicts the security clearance process during each phase, the organizations involved, and the technologies used during the process.



The DoD Security Clearance Process

For purposes of this audit, we focused on the Pre-Investigation Phase. During the Pre-Investigation Phase, individuals selected for employment complete the appropriate PSI forms[4] based on the level of clearance they require. The security and human resources personnel then review the PSI forms for accuracy and completeness, collect all the appropriate documentation, and submit the PSI request[5] to OPM via mail or e-QIP. OPM reviews the information for accuracy and completeness, coordinates with the requesting activity to correct erroneous data, and schedules the individual's PSI. For information regarding specific types of PSIs, levels of clearance, and required documentation, see Appendix C.

Technology Used in the Security Clearance Process. DoD implemented various technologies to improve the security clearance process, including JPAS, EPSQ, and e-QIP. JPAS is the official DoD personnel security system of record which provides real-time information regarding security clearances, access, and investigative status on DoD employees and contractors for security managers. EPSQ and e-QIP are software systems intended to automate the security clearance process. EPSQ allows individuals to electronically complete and validate information for PSIs. The e-QIP system enables individuals to create, edit,

[4] The PSI forms include the Standard Form 85, 85P, or 86, depending on the required level of clearance.

[5] The PSI request includes the appropriate Standard Form, as well as all other necessary documentation, such as the Fingerprint Card and Declaration of Federal Employment.

retrieve, update, and submit personnel investigative data as part of the PSI process. Individuals can initiate PSI requests via e-QIP through the JPAS system when authorized by their security manager. DoD intends to replace EPSQ with e-QIP to further automate the security clearance process, and, as of December 2005, had deployed e-QIP at select requesting activities in DoD.[6] Currently, e-QIP provides an online version of the SF 86, "Questionnaire for National Security Positions," and will soon provide other clearance forms.

Security Clearance Process Impediments at Requesting Activities

Requesting activities experienced difficulties in processing PSI requests for military and civilian personnel. Specifically, the difficulties included:

- inaccurate and incomplete personnel data,
- increased workloads for security managers,
- rejected PSI requests from OPM, and
- limited number of knowledgeable staff.

JPAS. JPAS allows security managers to verify clearance levels for personnel requiring access to sensitive and classified facilities and information. JPAS interfaces with at least 45 other DoD systems, including the Defense Eligibility Enrollment Reporting System and Defense Civilian Personnel Data System, to obtain military and civilian personnel information, respectively. JPAS data used by security managers to track personnel security clearances and periodic reinvestigations originate in JPAS via biweekly feeds from Defense Eligibility Enrollment Reporting System and Defense Civilian Personnel Data System. Based on access levels, JPAS allows users limited editing capabilities.

Reliability of Personnel Data. Security managers at 16 of the 26 requesting activities we visited stated that JPAS contained incomplete or inaccurate data on military and civilian employees. For example, at the Naval Education and Training Command, the security managers stated that JPAS did not contain information on PSIs older than 15 years. Navy policy requires individuals with confidential access to submit reinvestigation requests every 15 years. Therefore, if the security manager needed to verify investigation information for an individual with confidential access, JPAS might not contain a record for that individual, and the security manager would have to initiate the entire PSI process.

In addition, security personnel stated that JPAS contained data errors. Security personnel at Defense Logistics Agency Headquarters stated that JPAS reinvestigation reports often contained data inaccuracies, such as data for personnel separated from Government service and deceased personnel. Security

[6] The Office of Management and Budget has required DoD to implement e-QIP DoD-wide in April 2006.

personnel at European Command cited examples of multiple personnel with the same social security number and multiple social security numbers for one person. Additionally, security personnel at Camp Pendleton stated that information contained in JPAS reinvestigation reports sometimes conflicted with the information in the Defense Eligibility Enrollment Reporting System, which is one of the military personnel systems. Specifically, security personnel cited examples in which the Defense Eligibility Enrollment Reporting System continued to send information on retired personnel to JPAS, resulting in the individuals appearing on reinvestigation reports when they were no longer active DoD employees. Because security managers are responsible for tracking individuals' security clearances and contacting individuals for periodic reinvestigations, inaccurate reports can cause security mangers to spend unnecessary time researching and locating personnel who are no longer active DoD employees.

Correcting JPAS Data. Personnel from the JPAS Program Office stated the program offices that own the original data were responsible for the accuracy of the data because JPAS did not create the data, but downloaded data from other systems. Therefore, neither personnel from the JPAS Program Office nor security managers at requesting activities have direct access to correct inaccurate data. JPAS provides functionality for security managers to submit data correction requests to the appropriate program office; however, after submitting the request, security managers must wait for the program office to correct the data and feed it back into JPAS. Although JPAS provided functionality to correct data inaccuracies within the systems, security managers could not correct data in a timely manner, which forced security managers to work with inaccurate data.

Compensating Efforts by Requesting Activities. To overcome the inaccuracies in JPAS, security managers at 20 of the 26 requesting activities we visited created and maintained tandem systems to accurately track personnel security clearance information. The tandem systems ranged from simple Microsoft Excel spreadsheets to more elaborate security systems that combined several security functions, such as physical security and badge identification systems. Security managers highlighted three general reasons for maintaining tandem systems, including:

- inaccuracy of JPAS reinvestigation reports,
- inability to directly correct data inaccuracies, and
- lack of timely updates to personnel information.

At all 20 requesting activities, security managers entered duplicate information into JPAS and tandem systems, which increased the amount of work necessary to accurately track reinvestigations and security clearance levels.

Increased Workloads. Changes in guidelines for classifying information increased the amount of information that may be classified and the number of personnel needing security clearances. Executive Order 13292, dated March 25, 2003, provides guidelines for classifying information to defend against transnational terrorism, and increased the amount of information to be considered for classification over the previous Executive Order 12958, dated April 17, 1995.

Executive Order 13292 added functions related to the global war on terrorism, including logistics support, facilities, and infrastructures, in addition to those functions listed in Executive Order 12958, to be considered for classification. Additionally, GAO testimony in June 2005 stated that the increase in the operations and deployment of military personnel since September 11, 2001, and the sensitive technology that military personnel, Government civilians, and contractors use have impacted the personnel security clearance process. These situations have increased the number of personnel requiring access to classified information and the need for timely submission of PSI requests.

Security managers at requesting activities we visited repeated concerns of increased workloads. Specifically, the security manager at Defense Logistics Agency Enterprise Support Europe (DES-DE) stated that the number of personnel security clearances they process for one tenant increased from 5 in 2001 to 75 in 2003. Additionally, security personnel at the European Command explained that in the past, classified information was largely maintained at the senior officer level. However, in today's highly technologically oriented environment, more military personnel need access to classified information to drive a tank or program a weapon system to fire.

Rejected PSI Requests. All 26 requesting activities we visited experienced rejected PSI requests from OPM, which impacted the timeliness for processing security PSI requests. According to GAO testimony, in February 2005, OPM stated that about 11 percent of clearance investigation requests submitted outside the e-QIP system were returned to the requesting activity when missing or discrepant information could not be obtained by telephone. USD(I) personnel estimated that, as of April 2005, OPM rejected between 20 and 25 percent of DoD PSI requests. Although security managers at requesting activities implemented quality assurance procedures for reviewing and processing PSIs, OPM still rejected PSI requests due to incomplete or inaccurate data. Security managers stated that OPM established a process for correcting data inaccuracies prior to rejecting PSI requests; however, security managers provided several reasons why they could not fully comply with the process.

Quality Assurance Procedures at Requesting Activities. Security managers at requesting activities we visited seemed conscientious in reviewing the PSI requests for missing or inaccurate information before submitting to OPM. For example, security personnel at Ramstein Air Base in Germany reviewed PSI requests for completeness and accuracy twice before submitting to OPM: once at the unit security office and again at the base security office. Security personnel at Fort Stewart, when possible, met with individuals submitting PSI requests to review for accuracy and completeness of the PSI forms prior to submitting them to OPM. Additionally, security managers at the Space and Naval Warfare Command developed checklists to ensure that PSI requests contained all the appropriate documentation. However, security managers continued to receive rejected PSI requests due to inaccurate data such as outdated references, outdated phone numbers, outdated signatures, or inaccurate zip codes that may not be identified in a review for completeness. Security personnel at two security offices identified instances where OPM rejected the same PSI request three or four times due to inaccurate data. According to security managers, it appeared that OPM did not review the entire document and return it with all errors identified; rather, OPM returned the document when they identified one error. This process resulted in multiple rejections of PSI requests. These rejections contributed to delays in processing the PSI requests.

OPM Process for Addressing Errors. According to security managers at requesting activities we visited, OPM established procedures for its caseworkers to resolve any discrepancies on a PSI request. Generally, requesting activities had 3 days to respond to OPM with corrected information to avoid having OPM reject the PSI request. OPM rejected and returned the PSI request via mail if the caseworker could not contact the security manager or if the security manager could not respond with corrected data within 3 days.

Requesting Activities' Compliance With the OPM Process. Despite their efforts to resolve data discrepancies within 3 days, security managers cited several reasons for not fully complying with the OPM process. Security managers explained that the individuals to whom they provide personnel security services are not necessarily under their direct control, and the security managers may not be able to contact them within 3 days. For example, security managers at DES-DE provide security services to individuals in 85 countries throughout Europe. Therefore, if OPM contacted DES-DE to correct data inaccuracies, the DES-DE security manager may not necessarily have access to the individual to correct the information, or may not be able to contact the individual within the 3-day limit. Additionally, security personnel at Fort Huachuca stated that soldiers may be out on extended training exercises, and may not return within 3 days of OPM's initial contact. The security managers could not fully comply with the 3-day turnaround, and therefore received rejected PSI requests via mail.

Furthermore, security managers at requesting activities in Germany stated that they often did not receive phone calls or telephone messages from OPM. Security personnel at DES-DE attributed this condition to the time difference between the United States and Germany. In addition, one requesting activity we visited in Germany did not have voice mail or answering machines at its office. Specifically, security personnel at Ramstein Air Base stated that, in one instance, OPM mailed a rejected PSI request to the security office, noting that the caseworker left a telephone message regarding information on the PSI request, despite the security personnel not having voice mail or an answering machine. The security manager was not aware that the PSI request had been rejected until the request arrived in the mail. The 3-week timeframe for the requesting activities in Germany to receive the rejected PSI requests via mail significantly delays the process.

Improved Systems for Submitting PSI Requests. To reduce the number of rejected PSI requests from OPM, DoD began to use e-QIP, an OPM system that automates the process for completing, submitting, and scheduling PSIs. The e-QIP system is expected to improve the process for submitting PSI requests. DoD tested e-QIP at selected requesting activities. Out of 26 requesting activities we visited, only 2 used e-QIP to submit PSI requests. Security managers at Fort Huachuca and Ramstein Air Base stated that it took significantly less time for OPM to receive, schedule, and open an investigation when using e-QIP. Therefore, fully implementing e-QIP throughout DoD could increase the efficiency of processing PSI requests at the requesting activity level.

Best Practices. Security personnel at three requesting activities in Germany established procedures to efficiently work with OPM to resolve data inaccuracies. Specifically, security personnel at U.S Army Europe and the 6th Area Support Group, Germany, improved their ability to comply with the OPM timeline by attaching a memorandum to the front of each PSI request to have OPM caseworkers contact them via e-mail rather than by phone. The security personnel at Ramstein Air Base also verified that the process improved when they requested that OPM contact them via e-mail. The security manager at the 6th Area Support Group, Germany, established a good working relationship with the Branch Manager at OPM to resolve issues. Additionally, the security manager stated that all PSI requests submitted are screened by the Branch Manager's team, which helped in processing PSI requests and reduced the amount of rejected PSI requests.

Knowledgeable Staff. Despite making best efforts to perform their jobs, security managers responsible for timely and effectively processing PSIs, in some cases, lacked the experience, management support, or training to perform their duties most effectively. At the 26 requesting activities we visited, security personnel ranged from full-time experienced security managers with staffs, to military and/or civilian personnel completing security duties as collateral duties. For example, although the base security manager at Davis-Monthan Air Force Base was a full-time civilian whose primary duty was security, which includes personnel security, unit security managers were military personnel performing security responsibilities as collateral duties, often without prior personnel security experience.

Improvement Opportunities for Security Clearance Program

DoD requesting activities experienced difficulties in processing PSI requests for military and civilian personnel because USD(I) did not:

- establish minimum training requirements for security managers, or
- perform adequate management or oversight as required in DoD Regulation 5200.2-R.

In addition, USD(I), the Services, the Defense Information Systems Agency, and the Defense Logistics Agency did not consistently update policy to include complete information on eight key elements.

Adequacy of Training Requirements. DoD Regulation 5200.2-R does not include training requirements for security personnel to ensure a minimum level of training among all security personnel. Specifically, DoD Regulation 5200.2-R does not require security personnel to complete training on the personnel security clearance process. However, DoD has vehicles in place to offer personnel security clearance training. For example, the DSS Academy developed concentrations within the Security Disciplines, such as Counterintelligence, General Security, Information Security, and Personnel Security, and offers courses for security personnel aligned with each concentration. The Program

Management Concentration within the Personnel Security Discipline includes the following courses: Personnel Security Clearances, Personnel Security Management, and PSI Interface. In addition to training offered at DSS Academy, the Navy Security Training, Assistance, and Assessment Team (Pacific Command) and OPM provide training opportunities on the security clearance process and e-QIP, respectively.

Despite making best efforts to perform their jobs, some security personnel lacked the necessary training or experience, which may cause delays in the security clearance process. In addition, high personnel turnover at requesting activities contributed to inefficiencies in processing PSI requests.

Use of Security Training. Although DoD and OPM offer training for security personnel, security personnel did not consistently use the training throughout DoD for various reasons. Security managers at 11 requesting activities stated that they did not attend personnel security clearance training courses offered by the DSS Academy or other educational entities due to limited staffing within security offices, lack of training funds, or lack of training requirements. Therefore, security managers learned the security clearance process via on-the-job training or through briefing charts available at the requesting activity that outlined procedures for using security clearance systems, such as JPAS and e-QIP.

Although security managers may not have attended DoD or OPM training, security managers at five requesting activities developed standard operating procedures to aid security managers in processing PSI requests. These standard operating procedures outline specific procedures for processing PSI requests. For example, the Naval Education and Training Command developed and documented standard operating procedures that include process flowcharts and outline the step-by-step process for military and civilians personnel applying for clearances. Additionally, the Defense Information Systems Agency security office developed and documented standard operating procedures that clearly outline the personnel security clearance process and delegate responsibilities for processing PSI requests. Although these standard operating procedures are a viable tool for security managers without prior experience or training, they do not replace the need for personnel security training to ensure security managers receive the most updated information.

Personnel Turnover and Training Needs. Requesting activities we visited experienced high turnover for security managers, particularly when personnel security duties were performed by military personnel. For example, at Davis-Monthan Air Force Base the security manager stated that the turnover for unit security managers was very high due to changes in personnel duty stations. He stated that personnel turnover delayed the security clearance process because new unit security managers without prior experience or training must overcome a considerable learning curve to understand the security clearance process and the systems used to submit and track PSIs. Additionally, turnover of unit security managers at Fort Huachuca due to changes in duty stations contributed to delays in the security clearance process because new unit security managers often had no prior training or experience.

Turnover of personnel in security positions, in combination with recent changes to the security clearance program, including transition of investigative responsibilities from DSS to OPM and implementation of e-QIP and JPAS for processing PSI requests, increased the need for security managers to attend training. To effectively complete their security duties, security managers should be up-to-date on the personnel security clearance process and methods used to process PSI requests. DoD should establish minimum training requirements for security managers to obtain a broad knowledge base of the entire security clearance process, including the systems used to submit PSI requests and track clearance information. Required training will also help ensure a consistent level of knowledge among security managers, decrease delays in the security clearance process due to inexperienced personnel, and provide opportunities for disseminating updated information on the security clearance process.

Management and Oversight of the DoD Personnel Security Clearance Program. According to DoD Regulation 5200.2-R, USD(I) is to provide staff assistance to Services and Defense agencies on day-to-day security policy and operating problems and conduct inspections of DoD Components for compliance with DoD security policy and procedures. However, USD(I) stated that it was not able to provide the appropriate management and oversight of DoD Components due to limited staffing. Insufficient staffing limited the ability of USD(I) to monitor and communicate with requesting activities to provide updates as well as stay informed of concerns.

Limited Staffing at USD(I). The responsibility for the personnel security clearance program transitioned in May 2003 from the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence to USD(I). One person within the USD(I) Counterintelligence and Security Office was responsible for the DoD-wide personnel security clearance program for military, civilians, and contractors. As of September 2005, the Counterintelligence and Security Office expanded to include two contractor employees. According to DoD Regulation 5200.2-R, USD(I) is responsible for writing policy and guidance for the personnel security clearance program, and providing staff assistance for Services and Defense agencies to resolve policy and operating problems. USD(I) is also responsible for conducting inspections of Services and Defense agencies for compliance with DoD security policy and procedures. However, due to the limited staff, USD(I) had difficulty accomplishing this mission, specifically with updating policy in a timely fashion and providing oversight of the DoD-wide personnel security clearance program.

DSS Clearance Liaison Office. DSS, an agency of USD(I), established the DSS Clearance Liaison Office to support USD(I) with oversight, planning, developing, and communicating DoD policies regarding the personnel security clearance program, including coordinating and sponsoring OPM investigators conducting overseas interviews. The DSS Clearance Liaison Office, established in June 2005, is staffed with seven people functionally aligned with the Services, Defense agencies, and industry. However, security personnel at requesting activities we visited had limited, if any, knowledge of the establishment or responsibilities of the DSS Clearance Liaison Office. For example, the security manager at the Chief of Naval Operations stated that, although DSS announced the establishment of the office, they did not provide points of contact or other information for requesting activities to aid in the security clearance process. Security managers at three other requesting activities had limited knowledge of the establishment of the DSS Clearance Liaison Office, its mission, or points of contact.

Furthermore, the DSS Clearance Liaison Office did not adequately coordinate with security managers at requesting activities for the personnel security clearance process, specifically for overseas investigations. Security managers at requesting activities in Germany stated that OPM inexplicably ceased conducting overseas interviews from March 2005 through September 2005. As part of the transfer of the PSI function from DSS to OPM, DSS investigators became OPM employees. Consequently, OPM personnel explained that overseas interviews halted in March 2005 because OPM investigators did not have the authority to travel on DoD travel authorizations. DoD and OPM, therefore, established agreed-upon procedures, dated July 15, 2005, for OPM to complete overseas interviews for PSIs under DoD sponsorship. These procedures required OPM to provide at least 45 days notice before traveling overseas, and the OPM investigators arrived in Germany within approximately 60 days from the date of the agreement. However, security managers at requesting activities in Germany continued to experience what they considered to be inexplicable delays in obtaining security clearances.

Additionally, security managers at U.S. Army Europe and Ramstein Air Base stated that they did not receive adequate notice when OPM investigators conducted overseas interviews in September 2005. The security managers stated that they received notice only 1 day prior to the arrival of OPM investigators. As a result, security managers had to put forth a major effort to quickly locate and schedule PSI subject interviews for OPM investigators. Security managers stated that, had they received more advanced notice, they could have helped facilitate OPM investigations more efficiently by prioritizing and coordinating the necessary personnel for PSI interviews.

Other Management and Oversight Capabilities. Although USD(I) was not able to complete adequate management and oversight of the personnel security clearance program, DoD had mechanisms in place that could improve the oversight and management. Specifically, USD(I) held quarterly meetings of the Security Directors Group to discuss security issues and keep the DoD security community informed of current and future security policy initiatives. Additionally, Service and Defense agency policies require them to conduct regular inspections of requesting activities to measure compliance with security policies. These meetings and inspections could potentially help USD(I) accomplish their responsibility of management and oversight.

DoD Policy for the Personnel Security Clearance Program. DoD policies for the personnel security clearance program were outdated and contained incomplete information on the security clearance process. According to DoD Regulation 5200.2-R, USD(I) is responsible for writing policy and guidance for the personnel security clearance program. USD(I) originally anticipated issuing updated policy in October 2005; however, USD(I) had limited staffing and, as of January 2006, USD(I) had not issued updated policy.

The Services and Defense agencies we visited also have policies for the security clearance program; however, these policies were outdated and contained incomplete information on the security clearance process. Furthermore, Army, Navy, and Defense Information Systems Agency have not updated policies to include the transfer of investigative responsibilities from DSS to OPM, or security clearance systems used in the security clearance process. For example, although the Army published additional policy memorandums updating information on the security clearance process, the Army has not updated Army Regulation 380-67. The regulation, dated 1988, states that security managers should submit PSI requests to DSS via mail. However, current processes require security managers to submit PSI requests to OPM via mail. Army G-2 officials stated that the Army has not updated Army Regulation 380-67 because they want to update it based on the updated DoD Regulation 5200.2-R. Although the Air Force and Defense Logistics Agency updated their security clearance policies in 2005, the policies did not include complete information on the PSI submission processes, and the Defense Logistics Agency policy did not include information on types of PSIs or investigative scopes. Furthermore, the Defense Information Systems Agency policy did not provide a clear correlation between the levels of security clearance, the type of PSI necessary for each level of clearance, and the corresponding PSI forms required.

Based on site visits and discussions with security personnel at USD(I), the Services, the Defense agencies, and requesting activities, the eight key elements listed in the following table should be included in policy for requesting activities to effectively and efficiently process PSI requests. We evaluated DoD, Service, and Defense agency security policies for updated information regarding these key elements of the personnel security clearance process. The following table outlines whether the policies include information that does not need to be updated, include outdated or incomplete information, or did not include information on the key elements of the personnel security clearance process.

DoD, Service, and Defense Agency Personnel Security Policies and Analysis of Key Policy Elements

	Component and Year of Policy Publication					
Key Policy Elements	DoD 1987	Army 1988	Navy 1999	Air Force 2005	DISA 2002	DLA 2005
Program Management	Yellow	Yellow	Green	Green	Green	Green
Investigative Responsibilities	Yellow	Yellow	Yellow	Green	Red	Green
Security Clearance Systems	Yellow	Yellow	Yellow	Green	Red	Green
PSI Submission Processes	Yellow	Yellow	Yellow	Green	Red	Green
Types of PSIs	Yellow	Yellow	Yellow	Yellow	Red	Yellow
Investigative Scopes	Yellow	Yellow	Yellow	Yellow	Red	Yellow
Requirement for Compliance Inspections	Green	Green	Green	Green	Red	Green
Training Requirements	Red	Red	Red	Red	Red	Red

Green = Policy includes information that does not need to be updated

Yellow = Policy includes outdated or incomplete information

Red = Policy does not include information

More specifically, the key elements identified in the table above should include, for example, up to date information to identify:

- program management responsibilities for day-to-day management of the security clearance program;
- agencies responsible for conducting PSIs and investigative responsibilities;
- security clearance systems, which include the information technology systems such as JPAS, for tracking security clearance information;
- PSI submission processes;
- the relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI;
- requirements for compliance inspections, specifically compliance with personnel security policy; and
- training requirements for security personnel.

Security Clearance Delays and Potential Mission Impacts

As a result of difficulties submitting PSI requests, requesting activities may continue to experience delays in the security clearance process, thus increasing the timelines for obtaining a completed security clearance. Other potential effects of delays in the security clearance process include impacts to national security and the ability of DoD to complete critical missions and fully support the warfighter.

Specifically, delays in the security clearance process can result in negative consequences, such as nonproductive time while awaiting clearances. For example, delays have caused students at military training facilities to remain in a holdover status while waiting for a final clearance to complete training courses, graduate, or deploy. In addition, students without a final clearance may have their duty stations changed, which impacts their ability to fully support DoD missions for which they were trained.

Furthermore, a weak personnel security clearance process can impact our national security. Delays in the security clearance process can result in the loss of highly qualified candidates, and delays in the renewal of clearances for persons who already have access to classified information can lead to a heightened risk of disclosure of classified information. Delays in reinvestigations may lead to a heightened risk of national security breaches via unauthorized disclosure of classified information, which has the potential to cause exceptionally grave damage to national security.

Critical DoD Missions. Delays in the security clearance process may impact the ability of DoD to complete critical missions. Security managers at requesting activities in Germany cited examples where individuals without the appropriate level of security clearance arrived to complete classified work. However, until the security managers submitted the PSI requests and the individuals received the appropriate level of clearance, the individuals could not complete the work they were assigned.

Warfighter Support. Delays in the security clearance process may negatively impact overseas requesting activities' ability to support the warfighter. Information related to the global war on terrorism is often classified, requiring a large number of military and civilian personnel accessing the information to have clearances, especially in foreign countries. DoD cannot fully support the warfighter if it cannot send overseas individuals who have access to classified information.

This audit highlights continued shortcomings in overall program management, training requirements, and policy updates. Unless improved, these issues will continue to preclude DoD from increasing the efficiency and effectiveness, and from reducing delays in the personnel security clearance process. In August 2005, GAO responded to questions from Congress on the progress DoD has made to "develop and implement an integrated, comprehensive management plan to eliminate the backlog, reduce the delays in conducting investigations and determining eligibility for security clearances and overcome the impediments that could allow such problems to recur." GAO stated that it is unaware of any progress DoD had made and that DoD had not demonstrated development of an integrated approach for permanently eliminating the backlog and reducing delays. Therefore, by updating and publishing policy, establishing training requirements, and developing a plan for improving management and oversight, DoD will make steps toward improving the personnel security clearance process. USD(I) is taking steps to update DoD Regulation 5200.2-R; however, to improve the personnel security clearance process at Service and Defense agency levels, those organizations should coordinate with USD(I) and update their policies in the interim to more accurately reflect the changes to the process. Furthermore, these improvements should assist greatly in removing the DoD Security Clearance Program from the list of GAO high-risk areas.

Management Comments on Background

Under Secretary of Defense for Intelligence Comments on Adequacy of Management Controls and Self-Evaluation. The Acting Director of Security, Under Secretary of Defense for Intelligence commented on the management controls, stating that the organization has been working to improve the personnel security clearance process to support the 2.5 million military, civilian, and contractor personnel within DoD. The Acting Director stated that DoD has encountered lengthy times for investigations and adjudications due to funding and personnel shortfalls, but stated that it has made process improvements, such as transferring the investigative function to the Office of Personnel Management to maximize resources and centralize administration and oversight of personnel security investigations. The Acting Director also noted that other improvements were underway and that efforts were in place to accurately project workloads, submit all SF 86 forms electronically, and limit returned personnel security investigation requests.

Management Comments on Finding

Department of the Air Force Comments. The Director of Security Forces, Information Security commented on the finding, stating that Air Force Instruction 31-501 contained complete information on the personnel security clearance process, including program management responsibilities and personnel security investigation submission processes.

Audit Response. Air Force Instruction 31-501 lacked complete information on the types and scopes of personnel security investigations and did not include training requirements.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Under Secretary of Defense for Intelligence:

a. Update the DoD Regulation 5200.2-R, to:

(1) Include responsibilities of Under Secretary of Defense for Intelligence, the Defense Security Service Clearance Liaison Office, and the Office of Personnel Management in the areas of program management, oversight, and investigations;

(2) Define systems used for submitting and tracking security clearance information, such as the Joint Personnel Adjudication System and the Electronic Questionnaire for Investigations Processing;

(3) Define types of personnel security investigations, corresponding security clearance levels, and the required documentation; and

(4) Establish minimum training requirements for security personnel including, but not limited to, training on the security clearance process, the Joint Personnel Adjudication System, and the Electronic Questionnaire for Investigations Processing.

b. Establish milestones for publishing updated DoD Regulation 5200.2-R.

Under Secretary of Defense for Intelligence Comments. The Acting Director of Security, Under Secretary of Defense for Intelligence concurred, and stated that they plan to have a draft of the DoD Regulation 5200.2-R ready for staffing and coordination in July 2006, and expects to publish the updated regulation in summer 2007.

Defense Logistics Agency Comments. Although not required to comment, the Defense Logistics Agency concurred with the recommendation.

2. We recommend that the Under Secretary of Defense for Intelligence, in coordination with Services and Defense agencies, establish a vehicle to:

a. Improve communication of changes to the security clearance process between the Under Secretary of Defense for Intelligence and requesting activities;

b. Provide requesting activities a means to voice issues and for DoD and the Office of Personnel Management (as necessary) to expedite resolution; and

c. Identify processes and resources needed to improve oversight of the security clearance process at requesting activities, to include staff assistance.

Under Secretary of Defense for Intelligence Comments. The Acting Director of Security, Under Secretary of Defense for Intelligence concurred, stating that the organization is currently exploring options to best communicate with DoD Components on changes to the security clearance process and future plans, and to solicit input from field activities.

Defense Logistics Agency Comments. Although not required to comment, the Defense Logistics Agency concurred.

3. We recommend that the Army Deputy Chief of Staff for Intelligence; the Director, Naval Criminal Investigative Service; the Air Force Director of Security Forces, Information Security; the Director, Defense Information Systems Agency; and the Director, Defense Logistics Agency update policies for the DoD personnel security clearance program to include the following areas:

a. program management responsibilities;

b. agencies responsible for conducting PSIs and investigative responsibilities;

c. security clearance systems for tracking security clearance information;

d. PSI submission processes;

e. the relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI; and

f. training requirements for security personnel.

Department of the Army Comments. The Director, Counterintelligence, Human Intelligence, Disclosure, and Security Directorate for the Department of the Army, Office of the Deputy Chief of Staff, G-2 nonconcurred with Recommendations 3.a. through 3.e., and partially concurred with Recommendation 3.f. The Director stated that each of the critical elements listed in Recommendations 3.a. through 3.e. are provided in Army policy through memorandums and telephonic and e-mail communication to the Major Commands. Additionally, the Director indicated that they are coordinating with the Under Secretary of Defense and the Defense Security Service to develop a certification program for security professionals.

Audit Response. The Army comments are partially responsive. While the Army has met the intent of the recommendation by issuing memorandums to supplement Army Regulation 380-67, the Army should update the 1998 Army Regulation 380-67 to include current information on program management and investigative responsibilities, security clearance systems, training requirements, and submission processes, types, and scopes of personnel security investigations. We commend the Army for coordinating with the Under Secretary of Defense for Intelligence and the Defense Security Service to develop a certification program. However, we believe that training requirements should be included in the Army Regulation 380-67. We request the Army to reconsider its position on Recommendation 3. and provide additional comments in response to the final report.

Department of the Navy Comments. The Chief of Naval Operations, Special Assistant for Naval Investigations and Security (NO9N) partially concurred, stating that a Navy Personnel Security Program Policy Regulation is currently in draft and due for signature in May 2006. However, the Chief of Naval Operations did not provide information contained in the draft regulation, and stated that information regarding the responsibilities for conducting investigations, use of security clearance systems, PSI submission processes, and training requirements are located on the Chief of Naval Operations Web site.

Audit Response. The Navy comments are partially responsive. We commend the Navy for drafting a regulation for the Navy Personnel Security Program and agree that the Navy has issued and posted memorandums regarding responsibilities for conducting investigations, use of security clearance systems, and the PSI submission processes on the Chief of Naval Operations Web site. While the Navy's actions have met the intent of the recommendation, information on the investigative responsibilities, security clearance systems, and PSI submission processes should be included in the Navy Personnel Security Program policy. Therefore, we request that management provide additional information on the updated Navy policy, reconsider its position on Recommendation 3., and provide additional comments in response to the final report.

Department of the Air Force Comments. Although the Director of Security Forces, Information Security, commented on the finding, the Air Force did not comment on the recommendation. We request that the Air Force provide comments in response to the final report.

Defense Information Systems Agency Comments. The Director for Manpower, Personnel and Security concurred, stating that the Defense Information Systems Agency Instruction 240-110-8 is currently under revision and is estimated for completion in May 2006. The Director stated that information on investigative agencies, Personnel Security Investigation Submission process, and relationships among the levels of security clearances and types of personnel security investigations is outlined in the Defense Information Systems Agency Personnel Security Standard Operating Procedures. Additionally, the Director stated that the Defense Information Systems Agency developed a career management plan for all security specialists that details the required training suggested for career development and advancement.

Audit Response. The Defense Information Systems Agency comments are partially responsive. We commend the Defense Information Systems Agency for drafting an update to Defense Information Systems Agency Instruction 240-110-8; however, the Personnel Security Standard Operating Procedures should be included or referred to in the update to Defense Information Systems Agency Instruction 240-110-8. The updated Instruction should include information on the investigative agencies, the Personnel Security Investigation submission process, the relationships among the levels for security clearances and types of personnel security investigations and training requirements. Therefore, we request that the Defense Information Systems Agency provide additional information on the contents of the updated policy in response to the final report.

Defense Logistics Agency Comments. The Director, Defense Logistics Agency Enterprise Support, nonconcurred, stating that the Defense Logistics Agency One Book and Defense Logistics Agency Personnel Security Program Guidebook contain information on program management responsibilities, agencies responsible for conducting PSIs and investigative responsibilities, security clearance systems, the PSI submission process, levels of clearances, types of PSIs, and scopes and documentation required for PSIs. Additionally, the Director stated that the Defense Logistics Agency has not established written policy regarding training requirements because the Under Secretary of Defense for Intelligence has not issued training requirements. However, the Director noted that the Defense Logistics Agency has instituted internal training programs to train personnel security specialists on current issues, initiatives, security clearance systems, and other matters relative to personnel security.

Audit Response. The DLA comments are partially responsive. We agree that the DLA policy included complete and updated information on the program management responsibilities, investigative responsibilities, the security clearance systems, and the PSI submission process for the personnel security clearance process. However, the policy and guidance did not include complete and updated information on the types and scopes of PSIs and did not include information on the type or investigative scope of the Access National Agency Check with Inquiries or the Child Care National Agency Check and Inquiries. We commend the Defense Logistics Agency for implementing internal training programs to train personnel security specialists. While these actions meet the intent of the recommendation, training requirements should be included in Defense Logistics Agency policy. We request that management reconsider its position on Recommendation 3 and provide additional comments in response to the final report.

Appendix A. Scope and Methodology

We performed this audit from March 2005 through February 2006 in accordance with generally accepted government auditing standards. We evaluated the ability of DoD requesting activities to efficiently and effectively process security clearance requests. During site visits, we reviewed information regarding management of the security clearance program, roles and responsibilities of security manager, coordination among security and with human resources offices, information technology systems, training, and communication with investigative agencies. We interviewed officials from the USD(I), DoD Component headquarters, Defense agencies, and requesting activities from the Army, Navy, Air Force, and Marine Corps. We also reviewed documentation, including DoD, Service, Defense agency, and OPM policies, standard operating procedures, and documentation on JPAS. These documents ranged in dates from January 1987 through November 2005.

We visited officials at USD(I), Army G-2, Chief of Naval Operations, and the Director of Security Forces to gain information on the security clearance program at the Service level. We also visited DSS and the DSS Academy to gain information on JPAS and the training classes offered by DSS Academy. Finally, we met with an official from OPM to discuss investigative initiatives. Based on recommendations from DoD Component headquarters, we judgmentally selected 26 requesting activities that represented each of the Services and three Defense agencies. We visited and reviewed the security clearance programs at the following locations:

- U.S. European Command, Germany
- Army Materiel Command, Virginia
- U.S. Army Europe, Germany
- Fort Huachuca, Arizona
- Fort Stewart, Georgia
- 6th Area Support Group, Germany
- Human Resources Service Center Southwest, California
- Center for Information Dominance Corry Station, Florida
- Fleet Industrial Supply Center, California
- Naval Academy, Maryland
- Naval Air Station North Island, California
- Naval Air Station Pensacola, Florida

- Naval Criminal Investigative Service, Florida
- Naval Education and Training Command, Florida
- San Diego Broadway Complex, California
- Space and Naval Warfare Systems Command, California
- U.S. Air Force Europe, Germany
- Andrews Air Force Base, Maryland
- Davis-Monthan Air Force Base, Arizona
- Eglin Air Force Base, Florida
- Ramstein Air Base, Germany
- Camp Pendleton, California
- Defense Finance and Accounting Service, Virginia
- Defense Information Systems Agency, Virginia
- Defense Logistics Agency, Virginia
- Defense Logistics Agency Enterprise Support Europe, Germany

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of the DoD Personnel Security Clearance Program high-risk area.

Appendix B. Prior Coverage

During the last 5 years, GAO and the DoD Inspector General (IG) have issued 8 reports discussing DoD Personnel Security Clearance Program. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-05-842T, "Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges that Led to GAO's High-Risk Designation," June 28, 2005

GAO Report No. GAO-05-207, "High Risk Series," January 2005

GAO Report No. GAO-04-632, "Additional Steps Can Be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel," May 2004

GAO Report No. GAO-04-344, "DoD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size," February 2004

GAO Report No. GAO-01-465, "More Consistency Needed in Determining Eligibility for Top Secret Clearances," April 2001

DoD IG

DoD IG Report No. D-2001-136, "Defense Clearance and Investigations Index Database," June 7, 2001

DoD IG Report No. D-2001-112, "Acquisition Management of the Joint Personnel Adjudication System," May 5, 2001

DoD IG Report No. D-2001-065, "DoD Adjudication of Contractor Security Clearances Granted by the Defense Security Service," February 28, 2001

Appendix C. Types and Scopes of Personnel Security Investigations, Security Clearance Levels, and Required Documentation

The types of PSIs vary in scope of investigative effort required to meet the purpose of the particular investigation. DoD and OPM outline types of PSIs and corresponding security clearance levels, including but not limited to the following.

- **National Agency Check.** The National Agency Check (NAC) includes Federal Bureau of Investigation Name and Criminal History Fingerprint Checks, Defense Clearance Investigation Index search, and can include checks on military personnel records, citizenship, selective service, Central Intelligence Agency records, and State Department records.

- **NAC and Inquiries.** A NAC and Inquiries is the minimum investigation required for appointment to federal service. A NAC and Inquiries includes records checks associated with a NAC plus checks with law enforcement agencies, former employers and supervisors, residence, references, and schools covering the previous 3 to 5 years.

- **Child Care NAC and Inquiries.** A Child Care NAC and Inquiries is required for individuals holding positions within childcare facilities.

- **NAC With Law and Credit.** A NAC With Law and Credit is the minimal reinvestigation requirement for contractors or consultants for access to secret or confidential classified information. A NAC With Law and Credit includes all elements of NAC plus checks with law enforcements agencies for the last 5 years and credit checks for the last 7 years.

- **Access NAC With Inquiries.** An Access NAC With Inquiries is the minimum investigation required for secret or confidential clearance and includes all elements of the NACI, plus law enforcement and credit checks for the previous 5 to 7 years.

- **Single Scope Background Investigation.** A Single Scope Background Investigation is the investigation for individuals requiring a top secret clearance or working in a critical sensitive position. A Single Scope Background Investigation normally covers a 5-year period and consists of a subject interview, NAC, credit checks, character references, and employment records checks and references.

- **Reinvestigation.** Certain categories of duties, clearance, and access require the conduct of a reinvestigation every 5 to 15 years for military, civilian, contractor, and foreign nationals with access to classified material.

Required Documentation. Each level of security clearance requires different forms for PSIs. OPM requires the following standard forms and optional forms:

- SF-85 – Questionnaire for Non-Sensitive Positions
- SF-85P – Questionnaire for Public Trust Positions
- SF-86 – Questionnaire for National Security Positions
- SF-87 – Fingerprint Card (Federal Document 258 for contractors)
- Optional Form 306 – Declaration of Federal Employment

DoD, Service, and Defense agency policies dictate which forms to submit when requesting PSIs.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Intelligence

Department of the Army

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

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

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

Combatant Commands

Commander, U.S. European Command
Inspector General, U.S. Joint Forces Command

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Subcommittee on Personnel, Committee on Armed Services
Senate Subcommittee on Strategic Forces, Committee on Armed Services
Senate Subcommittee on Readiness and Management Support, Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
Senate Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Subcommittee on Total Force, Committee on Armed Services
House, Subcommittee on Readiness, Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform
House Permanent Select Committee on Intelligence

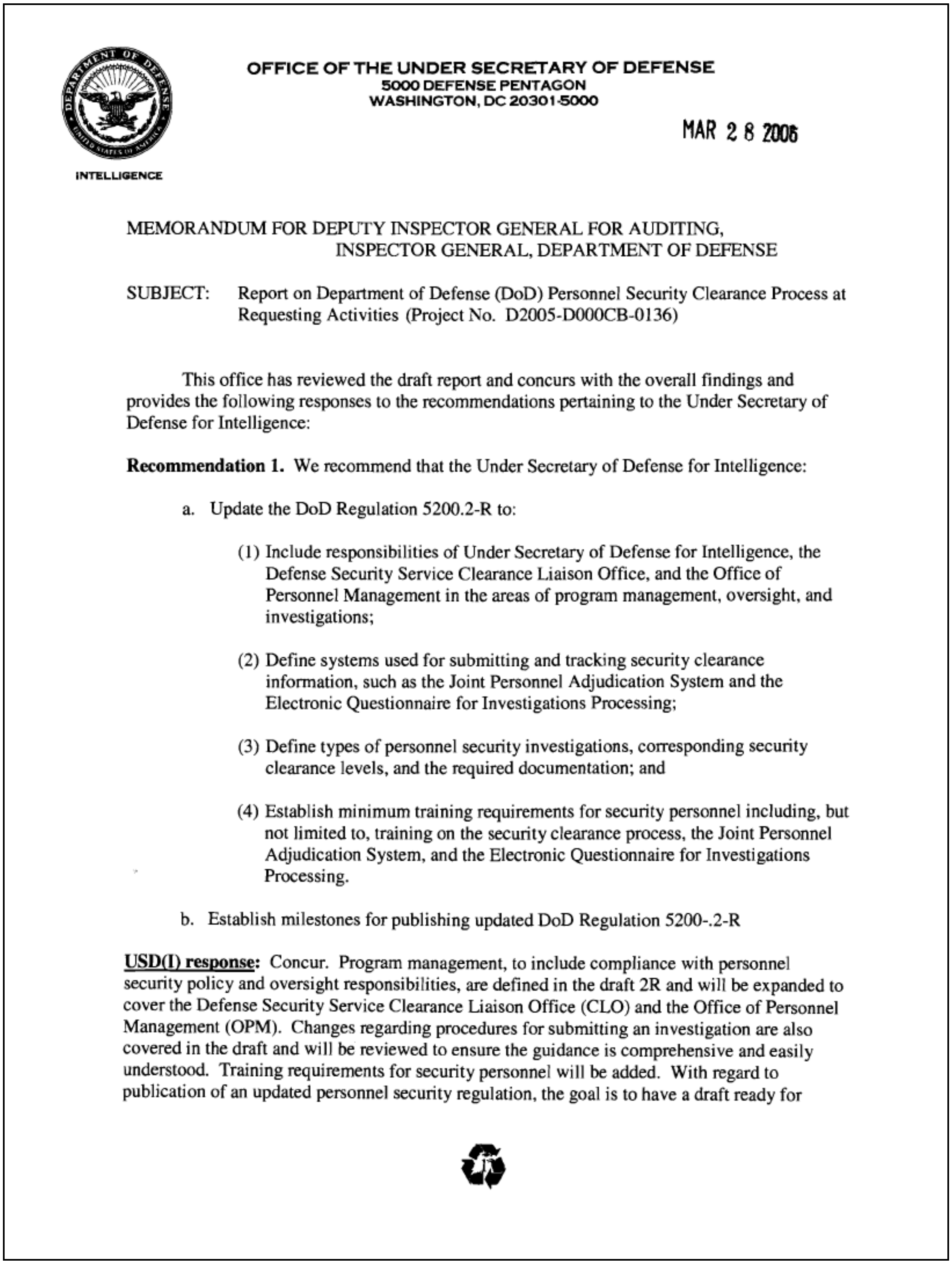
Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
Director, Defense Security Service

Non-Defense Federal Organization

Office of Management and Budget
Office of Personnel Management

Under Secretary of Defense for Intelligence Comments



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

MAR 28 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING,
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Report on Department of Defense (DoD) Personnel Security Clearance Process at Requesting Activities (Project No. D2005-D000CB-0136)

This office has reviewed the draft report and concurs with the overall findings and provides the following responses to the recommendations pertaining to the Under Secretary of Defense for Intelligence:

Recommendation 1. We recommend that the Under Secretary of Defense for Intelligence:

a. Update the DoD Regulation 5200.2-R to:

(1) Include responsibilities of Under Secretary of Defense for Intelligence, the Defense Security Service Clearance Liaison Office, and the Office of Personnel Management in the areas of program management, oversight, and investigations;

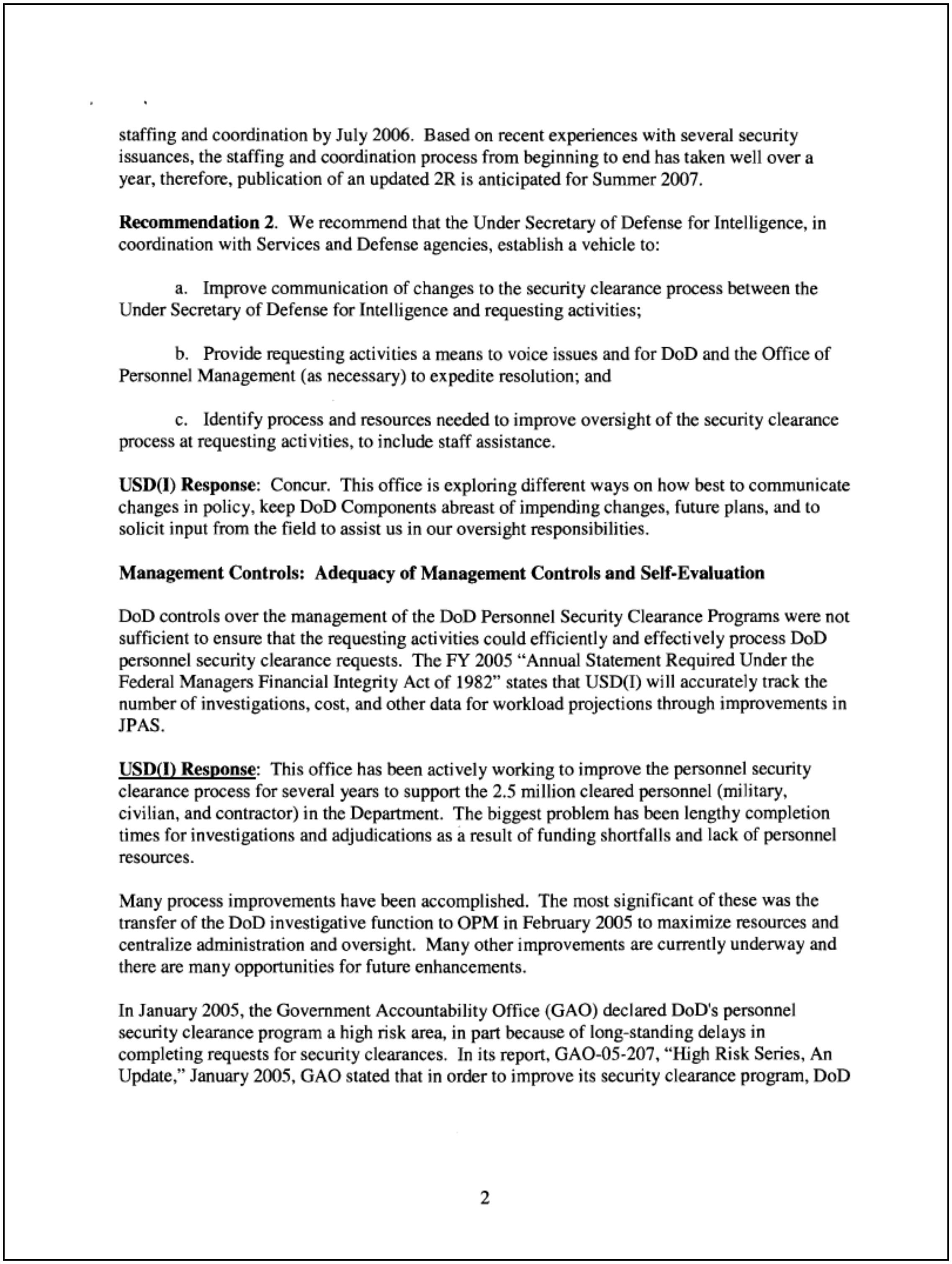
(2) Define systems used for submitting and tracking security clearance information, such as the Joint Personnel Adjudication System and the Electronic Questionnaire for Investigations Processing;

(3) Define types of personnel security investigations, corresponding security clearance levels, and the required documentation; and

(4) Establish minimum training requirements for security personnel including, but not limited to, training on the security clearance process, the Joint Personnel Adjudication System, and the Electronic Questionnaire for Investigations Processing.

b. Establish milestones for publishing updated DoD Regulation 5200-.2-R

USD(I) response: Concur. Program management, to include compliance with personnel security policy and oversight responsibilities, are defined in the draft 2R and will be expanded to cover the Defense Security Service Clearance Liaison Office (CLO) and the Office of Personnel Management (OPM). Changes regarding procedures for submitting an investigation are also covered in the draft and will be reviewed to ensure the guidance is comprehensive and easily understood. Training requirements for security personnel will be added. With regard to publication of an updated personnel security regulation, the goal is to have a draft ready for



staffing and coordination by July 2006. Based on recent experiences with several security issuances, the staffing and coordination process from beginning to end has taken well over a year, therefore, publication of an updated 2R is anticipated for Summer 2007.

Recommendation 2. We recommend that the Under Secretary of Defense for Intelligence, in coordination with Services and Defense agencies, establish a vehicle to:

a. Improve communication of changes to the security clearance process between the Under Secretary of Defense for Intelligence and requesting activities;

b. Provide requesting activities a means to voice issues and for DoD and the Office of Personnel Management (as necessary) to expedite resolution; and

c. Identify process and resources needed to improve oversight of the security clearance process at requesting activities, to include staff assistance.

USD(I) Response: Concur. This office is exploring different ways on how best to communicate changes in policy, keep DoD Components abreast of impending changes, future plans, and to solicit input from the field to assist us in our oversight responsibilities.

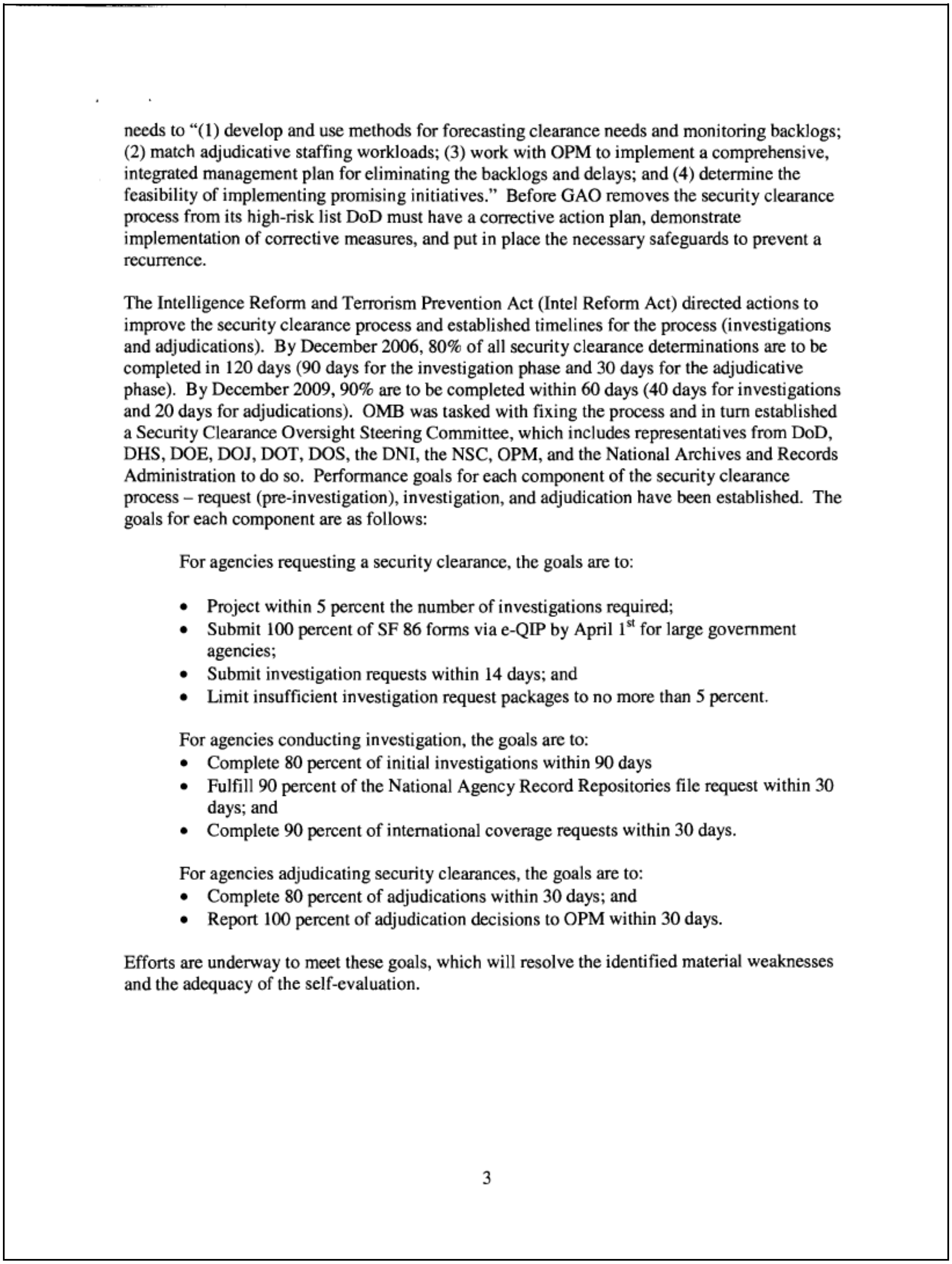
Management Controls: Adequacy of Management Controls and Self-Evaluation

DoD controls over the management of the DoD Personnel Security Clearance Programs were not sufficient to ensure that the requesting activities could efficiently and effectively process DoD personnel security clearance requests. The FY 2005 "Annual Statement Required Under the Federal Managers Financial Integrity Act of 1982" states that USD(I) will accurately track the number of investigations, cost, and other data for workload projections through improvements in JPAS.

USD(I) Response: This office has been actively working to improve the personnel security clearance process for several years to support the 2.5 million cleared personnel (military, civilian, and contractor) in the Department. The biggest problem has been lengthy completion times for investigations and adjudications as a result of funding shortfalls and lack of personnel resources.

Many process improvements have been accomplished. The most significant of these was the transfer of the DoD investigative function to OPM in February 2005 to maximize resources and centralize administration and oversight. Many other improvements are currently underway and there are many opportunities for future enhancements.

In January 2005, the Government Accountability Office (GAO) declared DoD's personnel security clearance program a high risk area, in part because of long-standing delays in completing requests for security clearances. In its report, GAO-05-207, "High Risk Series, An Update," January 2005, GAO stated that in order to improve its security clearance program, DoD



needs to "(1) develop and use methods for forecasting clearance needs and monitoring backlogs; (2) match adjudicative staffing workloads; (3) work with OPM to implement a comprehensive, integrated management plan for eliminating the backlogs and delays; and (4) determine the feasibility of implementing promising initiatives." Before GAO removes the security clearance process from its high-risk list DoD must have a corrective action plan, demonstrate implementation of corrective measures, and put in place the necessary safeguards to prevent a recurrence.

The Intelligence Reform and Terrorism Prevention Act (Intel Reform Act) directed actions to improve the security clearance process and established timelines for the process (investigations and adjudications). By December 2006, 80% of all security clearance determinations are to be completed in 120 days (90 days for the investigation phase and 30 days for the adjudicative phase). By December 2009, 90% are to be completed within 60 days (40 days for investigations and 20 days for adjudications). OMB was tasked with fixing the process and in turn established a Security Clearance Oversight Steering Committee, which includes representatives from DoD, DHS, DOE, DOJ, DOT, DOS, the DNI, the NSC, OPM, and the National Archives and Records Administration to do so. Performance goals for each component of the security clearance process – request (pre-investigation), investigation, and adjudication have been established. The goals for each component are as follows:

For agencies requesting a security clearance, the goals are to:

- Project within 5 percent the number of investigations required;
- Submit 100 percent of SF 86 forms via e-QIP by April 1st for large government agencies;
- Submit investigation requests within 14 days; and
- Limit insufficient investigation request packages to no more than 5 percent.

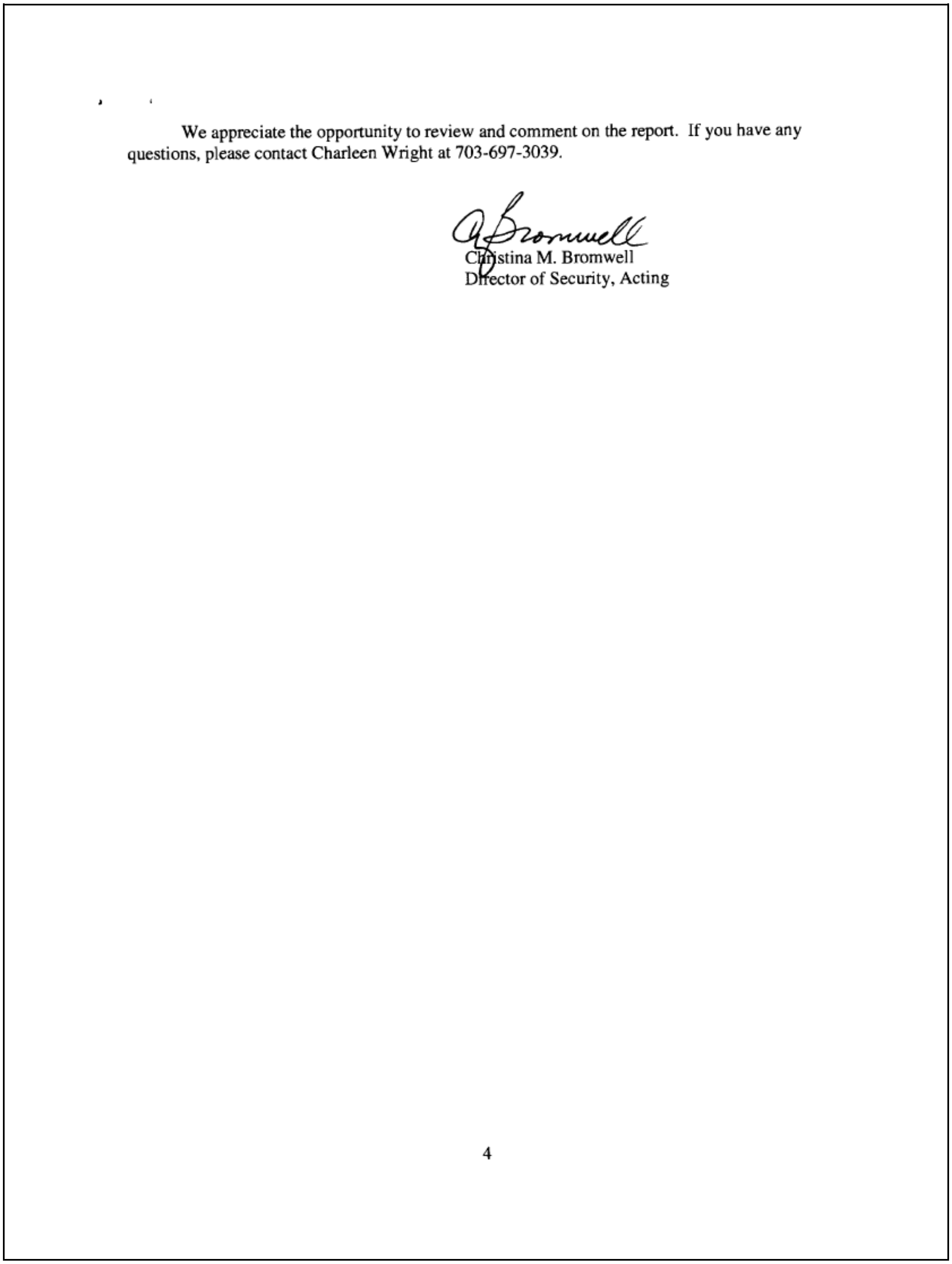
For agencies conducting investigation, the goals are to:

- Complete 80 percent of initial investigations within 90 days
- Fulfill 90 percent of the National Agency Record Repositories file request within 30 days; and
- Complete 90 percent of international coverage requests within 30 days.

For agencies adjudicating security clearances, the goals are to:

- Complete 80 percent of adjudications within 30 days; and
- Report 100 percent of adjudication decisions to OPM within 30 days.

Efforts are underway to meet these goals, which will resolve the identified material weaknesses and the adequacy of the self-evaluation.

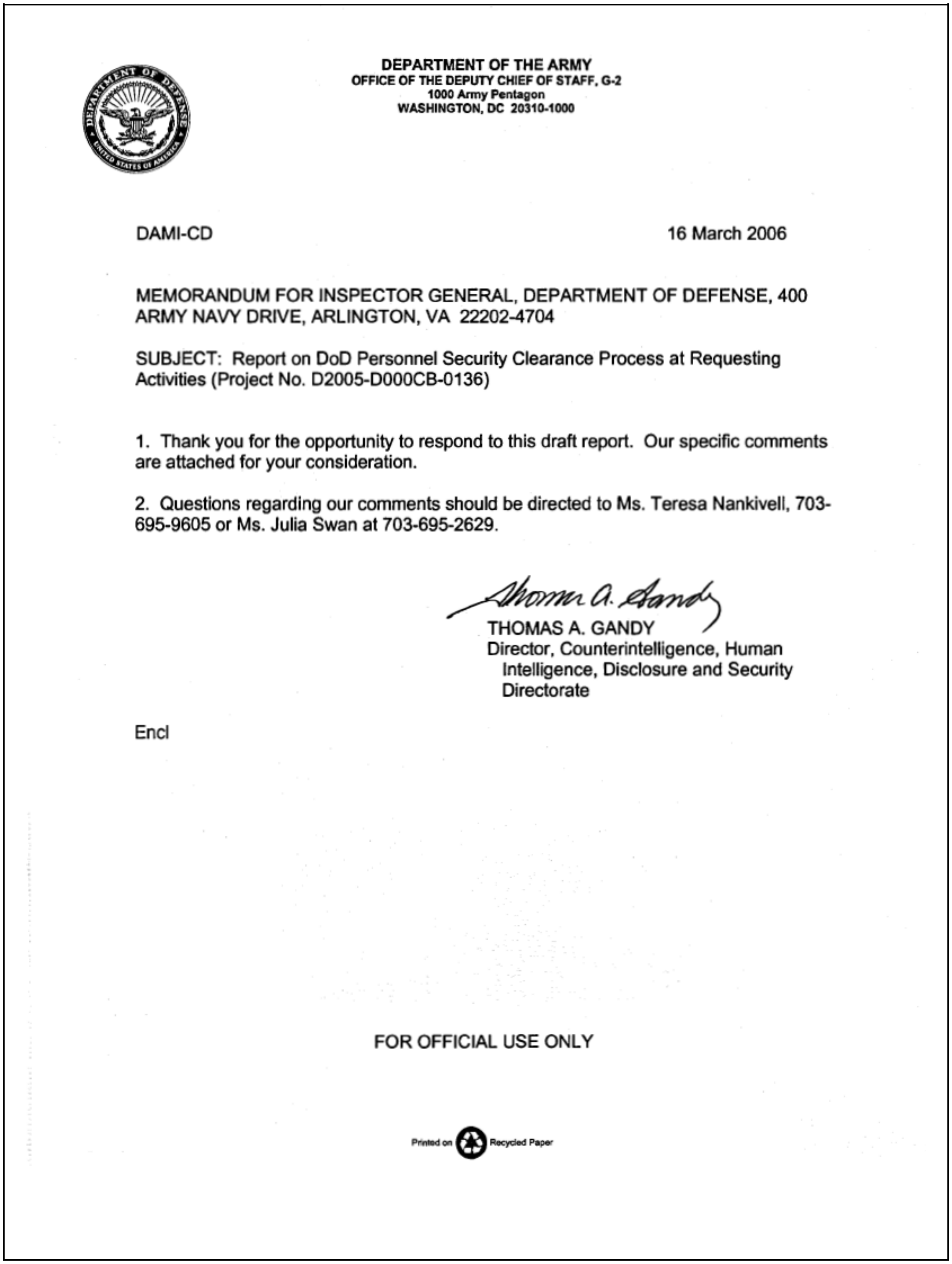


We appreciate the opportunity to review and comment on the report. If you have any questions, please contact Charleen Wright at 703-697-3039.

C Bromwell

Christina M. Bromwell
Director of Security, Acting

Department of the Army Comments



DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 Army Pentagon
WASHINGTON, DC 20310-1000

DAMI-CD

16 March 2006

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, 400 ARMY NAVY DRIVE, ARLINGTON, VA 22202-4704

SUBJECT: Report on DoD Personnel Security Clearance Process at Requesting Activities (Project No. D2005-D000CB-0136)

1. Thank you for the opportunity to respond to this draft report. Our specific comments are attached for your consideration.

2. Questions regarding our comments should be directed to Ms. Teresa Nankivell, 703-695-9605 or Ms. Julia Swan at 703-695-2629.

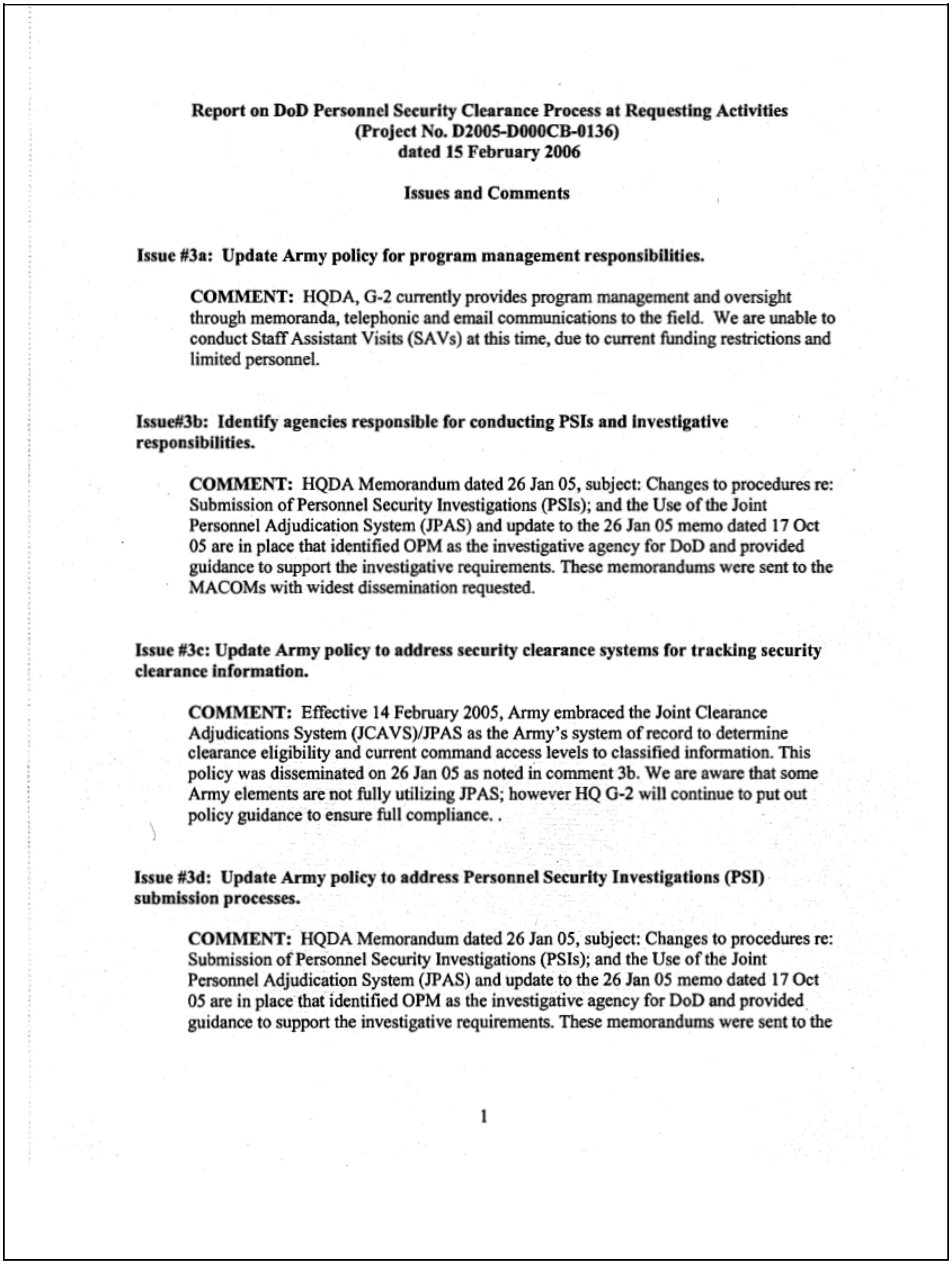
Thomas A. Gandy

THOMAS A. GANDY
Director, Counterintelligence, Human
Intelligence, Disclosure and Security
Directorate

Encl

FOR OFFICIAL USE ONLY

Printed on Recycled Paper



Report on DoD Personnel Security Clearance Process at Requesting Activities
(Project No. D2005-D000CB-0136)
dated 15 February 2006

Issues and Comments

Issue #3a: Update Army policy for program management responsibilities.

COMMENT: HQDA, G-2 currently provides program management and oversight through memoranda, telephonic and email communications to the field. We are unable to conduct Staff Assistant Visits (SAVs) at this time, due to current funding restrictions and limited personnel.

Issue#3b: Identify agencies responsible for conducting PSIs and investigative responsibilities.

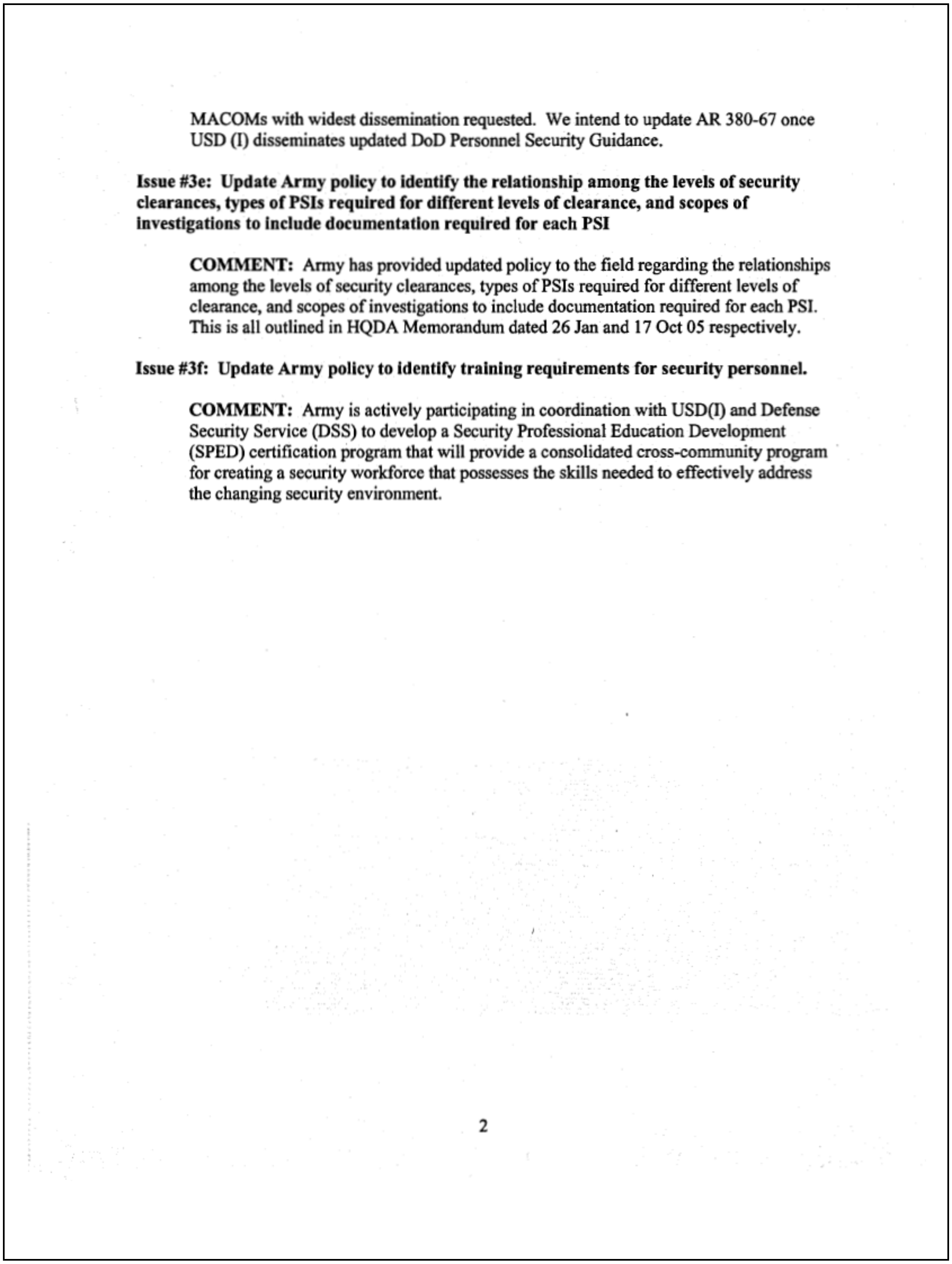
COMMENT: HQDA Memorandum dated 26 Jan 05, subject: Changes to procedures re: Submission of Personnel Security Investigations (PSIs); and the Use of the Joint Personnel Adjudication System (JPAS) and update to the 26 Jan 05 memo dated 17 Oct 05 are in place that identified OPM as the investigative agency for DoD and provided guidance to support the investigative requirements. These memorandums were sent to the MACOMs with widest dissemination requested.

Issue #3c: Update Army policy to address security clearance systems for tracking security clearance information.

COMMENT: Effective 14 February 2005, Army embraced the Joint Clearance Adjudications System (JCAVS)/JPAS as the Army's system of record to determine clearance eligibility and current command access levels to classified information. This policy was disseminated on 26 Jan 05 as noted in comment 3b. We are aware that some Army elements are not fully utilizing JPAS; however HQ G-2 will continue to put out policy guidance to ensure full compliance. .

Issue #3d: Update Army policy to address Personnel Security Investigations (PSI) submission processes.

COMMENT: HQDA Memorandum dated 26 Jan 05, subject: Changes to procedures re: Submission of Personnel Security Investigations (PSIs); and the Use of the Joint Personnel Adjudication System (JPAS) and update to the 26 Jan 05 memo dated 17 Oct 05 are in place that identified OPM as the investigative agency for DoD and provided guidance to support the investigative requirements. These memorandums were sent to the



MACOMs with widest dissemination requested. We intend to update AR 380-67 once USD (I) disseminates updated DoD Personnel Security Guidance.

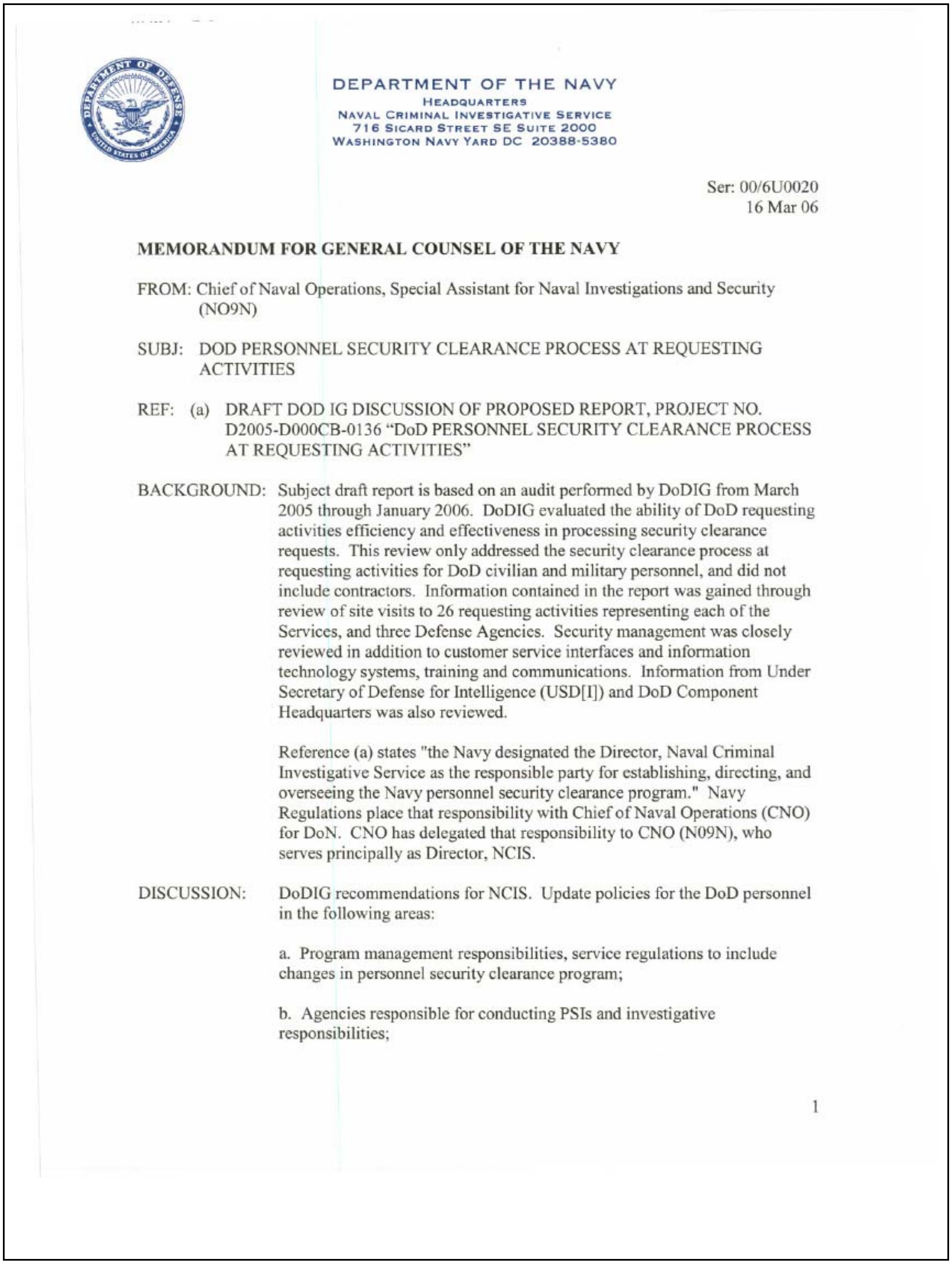
Issue #3e: Update Army policy to identify the relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI

COMMENT: Army has provided updated policy to the field regarding the relationships among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI. This is all outlined in HQDA Memorandum dated 26 Jan and 17 Oct 05 respectively.

Issue #3f: Update Army policy to identify training requirements for security personnel.

COMMENT: Army is actively participating in coordination with USD(I) and Defense Security Service (DSS) to develop a Security Professional Education Development (SPED) certification program that will provide a consolidated cross-community program for creating a security workforce that possesses the skills needed to effectively address the changing security environment.

Department of the Navy Comments



DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
716 SICARD STREET SE SUITE 2000
WASHINGTON NAVY YARD DC 20388-5380

Ser: 00/6U0020
16 Mar 06

MEMORANDUM FOR GENERAL COUNSEL OF THE NAVY

FROM: Chief of Naval Operations, Special Assistant for Naval Investigations and Security (NO9N)

SUBJ: DOD PERSONNEL SECURITY CLEARANCE PROCESS AT REQUESTING ACTIVITIES

REF: (a) DRAFT DOD IG DISCUSSION OF PROPOSED REPORT, PROJECT NO. D2005-D000CB-0136 "DoD PERSONNEL SECURITY CLEARANCE PROCESS AT REQUESTING ACTIVITIES"

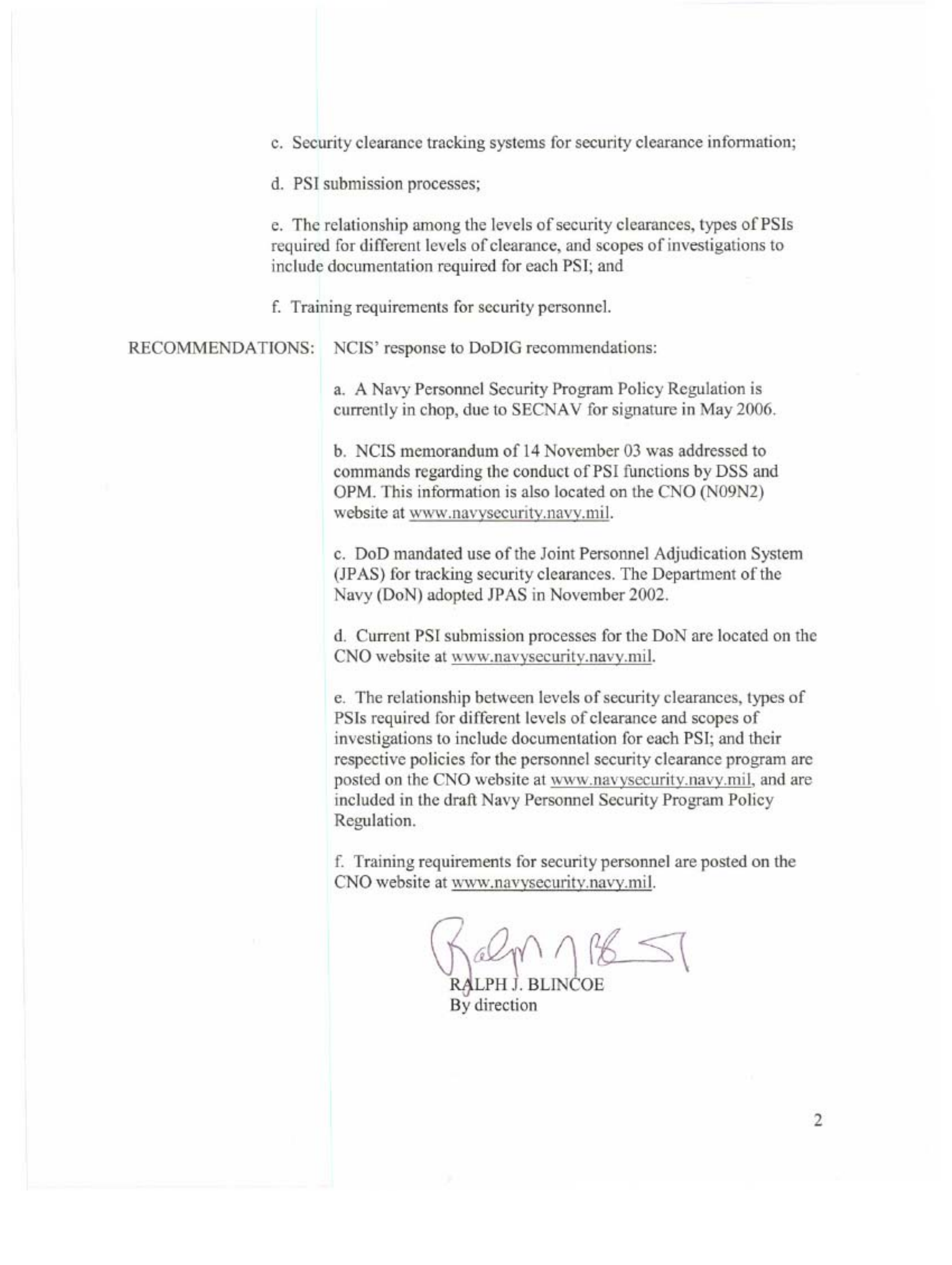
BACKGROUND: Subject draft report is based on an audit performed by DoDIG from March 2005 through January 2006. DoDIG evaluated the ability of DoD requesting activities efficiency and effectiveness in processing security clearance requests. This review only addressed the security clearance process at requesting activities for DoD civilian and military personnel, and did not include contractors. Information contained in the report was gained through review of site visits to 26 requesting activities representing each of the Services, and three Defense Agencies. Security management was closely reviewed in addition to customer service interfaces and information technology systems, training and communications. Information from Under Secretary of Defense for Intelligence (USD[I]) and DoD Component Headquarters was also reviewed.

Reference (a) states "the Navy designated the Director, Naval Criminal Investigative Service as the responsible party for establishing, directing, and overseeing the Navy personnel security clearance program." Navy Regulations place that responsibility with Chief of Naval Operations (CNO) for DoN. CNO has delegated that responsibility to CNO (N09N), who serves principally as Director, NCIS.

DISCUSSION: DoDIG recommendations for NCIS. Update policies for the DoD personnel in the following areas:

a. Program management responsibilities, service regulations to include changes in personnel security clearance program;

b. Agencies responsible for conducting PSIs and investigative responsibilities;



c. Security clearance tracking systems for security clearance information;

d. PSI submission processes;

e. The relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI; and

f. Training requirements for security personnel.

RECOMMENDATIONS: NCIS' response to DoDIG recommendations:

a. A Navy Personnel Security Program Policy Regulation is currently in chop, due to SECNAV for signature in May 2006.

b. NCIS memorandum of 14 November 03 was addressed to commands regarding the conduct of PSI functions by DSS and OPM. This information is also located on the CNO (N09N2) website at www.navysecurity.navy.mil.

c. DoD mandated use of the Joint Personnel Adjudication System (JPAS) for tracking security clearances. The Department of the Navy (DoN) adopted JPAS in November 2002.

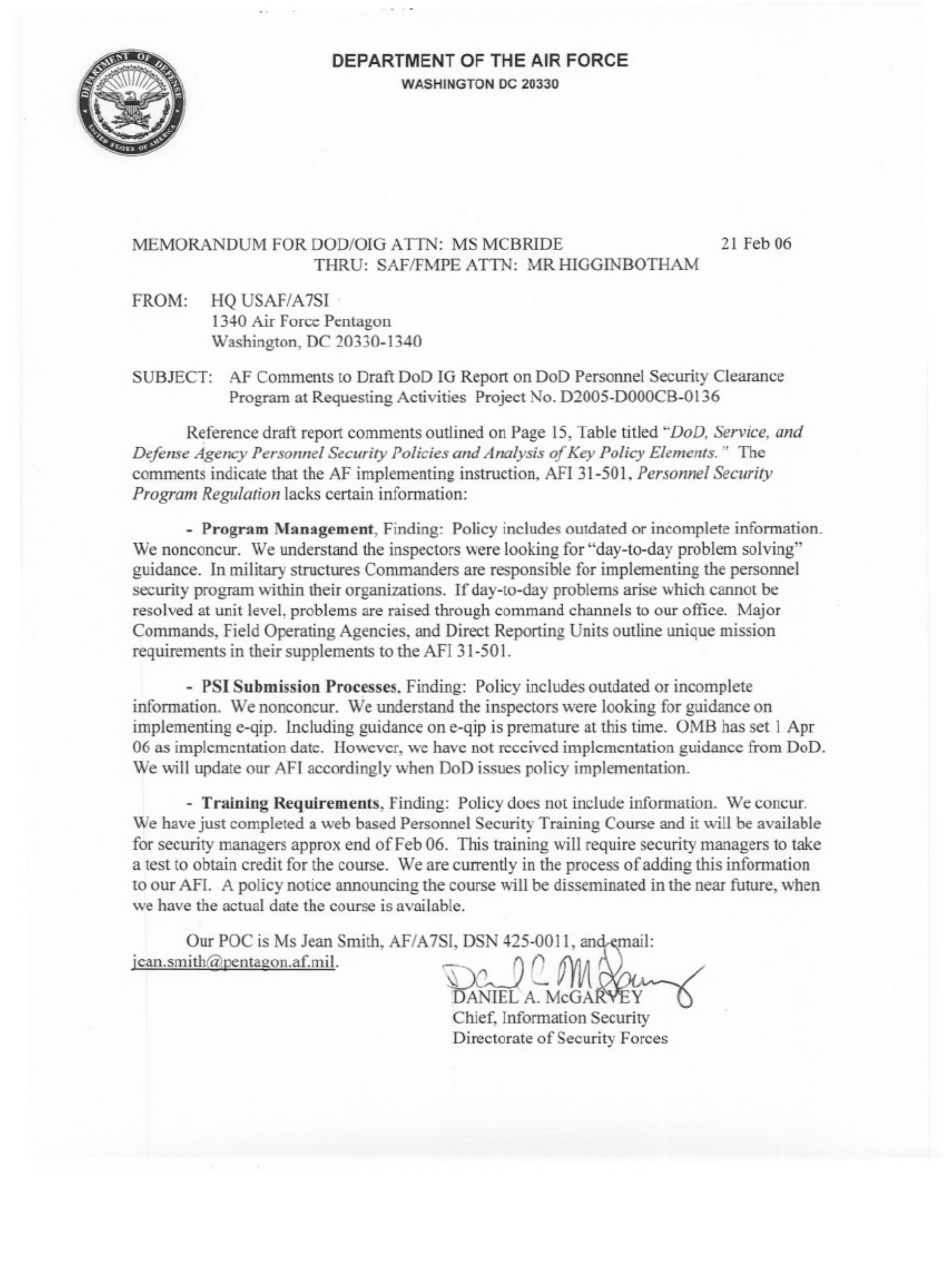
d. Current PSI submission processes for the DoN are located on the CNO website at www.navysecurity.navy.mil.

e. The relationship between levels of security clearances, types of PSIs required for different levels of clearance and scopes of investigations to include documentation for each PSI; and their respective policies for the personnel security clearance program are posted on the CNO website at www.navysecurity.navy.mil, and are included in the draft Navy Personnel Security Program Policy Regulation.

f. Training requirements for security personnel are posted on the CNO website at www.navysecurity.navy.mil.

RALPH J. BLINCOE
By direction

Department of the Air Force Comments



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330

MEMORANDUM FOR DOD/OIG ATTN: MS MCBRIDE 21 Feb 06
THRU: SAF/FMPE ATTN: MR HIGGINBOTHAM

FROM: HQ USAF/A7SI
1340 Air Force Pentagon
Washington, DC 20330-1340

SUBJECT: AF Comments to Draft DoD IG Report on DoD Personnel Security Clearance Program at Requesting Activities Project No. D2005-D000CB-0136

Reference draft report comments outlined on Page 15, Table titled "*DoD, Service, and Defense Agency Personnel Security Policies and Analysis of Key Policy Elements.*" The comments indicate that the AF implementing instruction, AFI 31-501, *Personnel Security Program Regulation* lacks certain information:

- **Program Management**, Finding: Policy includes outdated or incomplete information. We nonconcur. We understand the inspectors were looking for "day-to-day problem solving" guidance. In military structures Commanders are responsible for implementing the personnel security program within their organizations. If day-to-day problems arise which cannot be resolved at unit level, problems are raised through command channels to our office. Major Commands, Field Operating Agencies, and Direct Reporting Units outline unique mission requirements in their supplements to the AFI 31-501.

- **PSI Submission Processes**, Finding: Policy includes outdated or incomplete information. We nonconcur. We understand the inspectors were looking for guidance on implementing e-qip. Including guidance on e-qip is premature at this time. OMB has set 1 Apr 06 as implementation date. However, we have not received implementation guidance from DoD. We will update our AFI accordingly when DoD issues policy implementation.

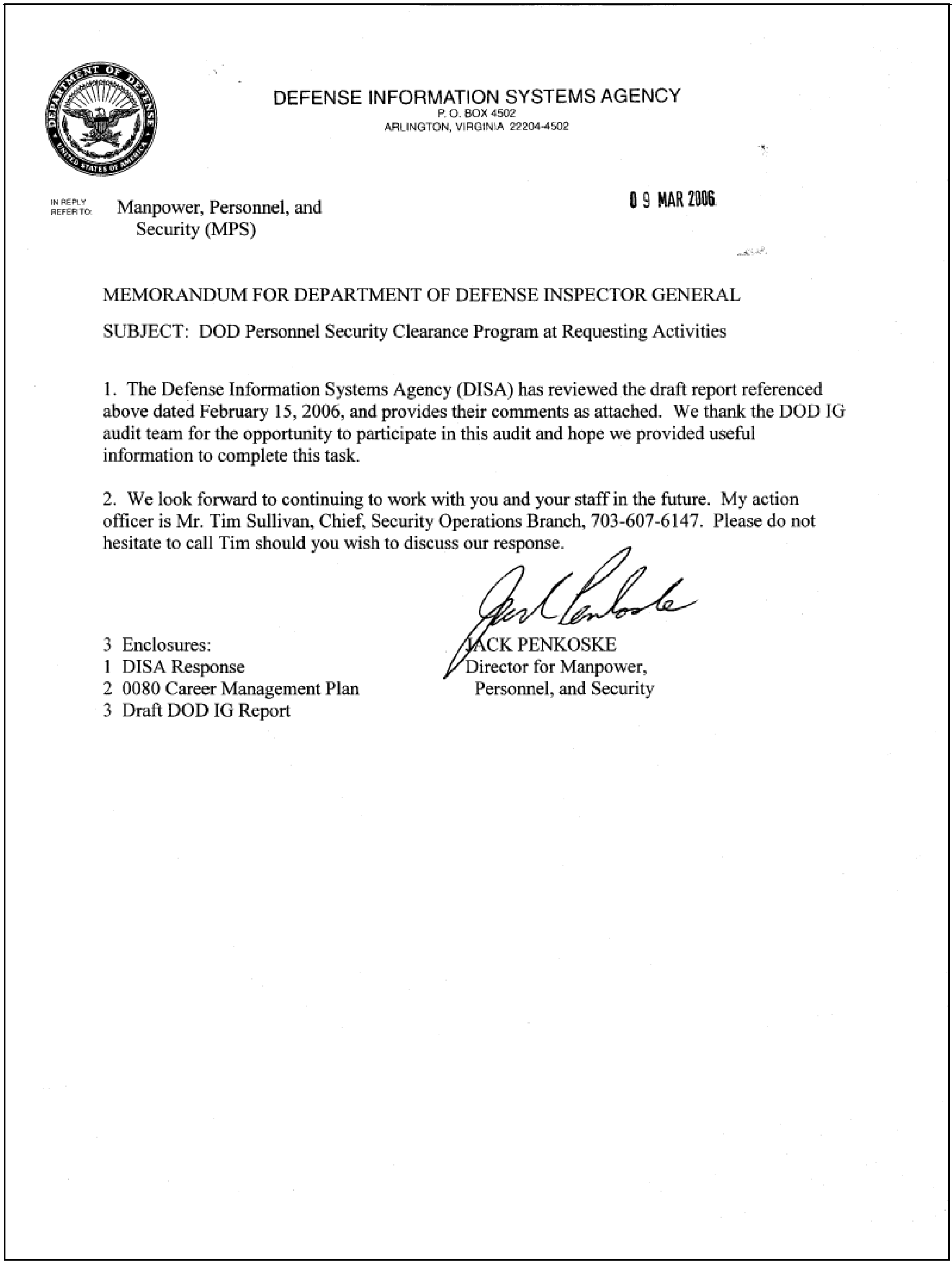
- **Training Requirements**, Finding: Policy does not include information. We concur. We have just completed a web based Personnel Security Training Course and it will be available for security managers approx end of Feb 06. This training will require security managers to take a test to obtain credit for the course. We are currently in the process of adding this information to our AFI. A policy notice announcing the course will be disseminated in the near future, when we have the actual date the course is available.

Our POC is Ms Jean Smith, AF/A7SI, DSN 425-0011, and email: jean.smith@pentagon.af.mil.

DANIEL A. McGARVEY
Chief, Information Security
Directorate of Security Forces

Defense Information Systems Agency Comments

Final Report
Reference



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Manpower, Personnel, and
Security (MPS)

0 9 MAR 2006

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DOD Personnel Security Clearance Program at Requesting Activities

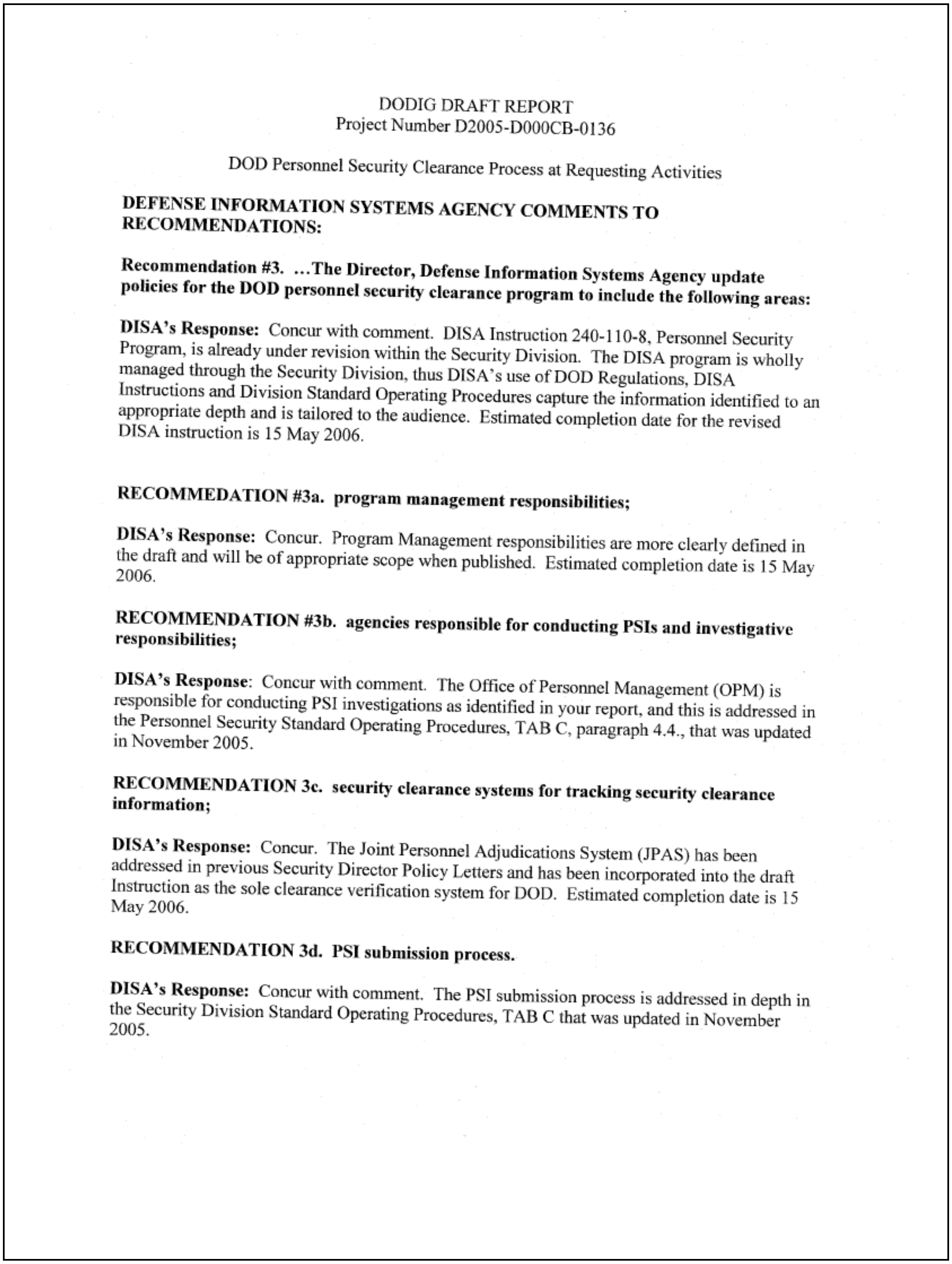
1. The Defense Information Systems Agency (DISA) has reviewed the draft report referenced above dated February 15, 2006, and provides their comments as attached. We thank the DOD IG audit team for the opportunity to participate in this audit and hope we provided useful information to complete this task.

2. We look forward to continuing to work with you and your staff in the future. My action officer is Mr. Tim Sullivan, Chief, Security Operations Branch, 703-607-6147. Please do not hesitate to call Tim should you wish to discuss our response.

JACK PENKOSKE
Director for Manpower,
Personnel, and Security

3 Enclosures:
1 DISA Response
2 0080 Career Management Plan
3 Draft DOD IG Report

Omitted enclosures 2 and 3 due to length.



DODIG DRAFT REPORT
Project Number D2005-D000CB-0136

DOD Personnel Security Clearance Process at Requesting Activities

DEFENSE INFORMATION SYSTEMS AGENCY COMMENTS TO RECOMMENDATIONS:

Recommendation #3. …The Director, Defense Information Systems Agency update policies for the DOD personnel security clearance program to include the following areas:

DISA's Response: Concur with comment. DISA Instruction 240-110-8, Personnel Security Program, is already under revision within the Security Division. The DISA program is wholly managed through the Security Division, thus DISA's use of DOD Regulations, DISA Instructions and Division Standard Operating Procedures capture the information identified to an appropriate depth and is tailored to the audience. Estimated completion date for the revised DISA instruction is 15 May 2006.

RECOMMEDATION #3a. program management responsibilities;

DISA's Response: Concur. Program Management responsibilities are more clearly defined in the draft and will be of appropriate scope when published. Estimated completion date is 15 May 2006.

RECOMMENDATION #3b. agencies responsible for conducting PSIs and investigative responsibilities;

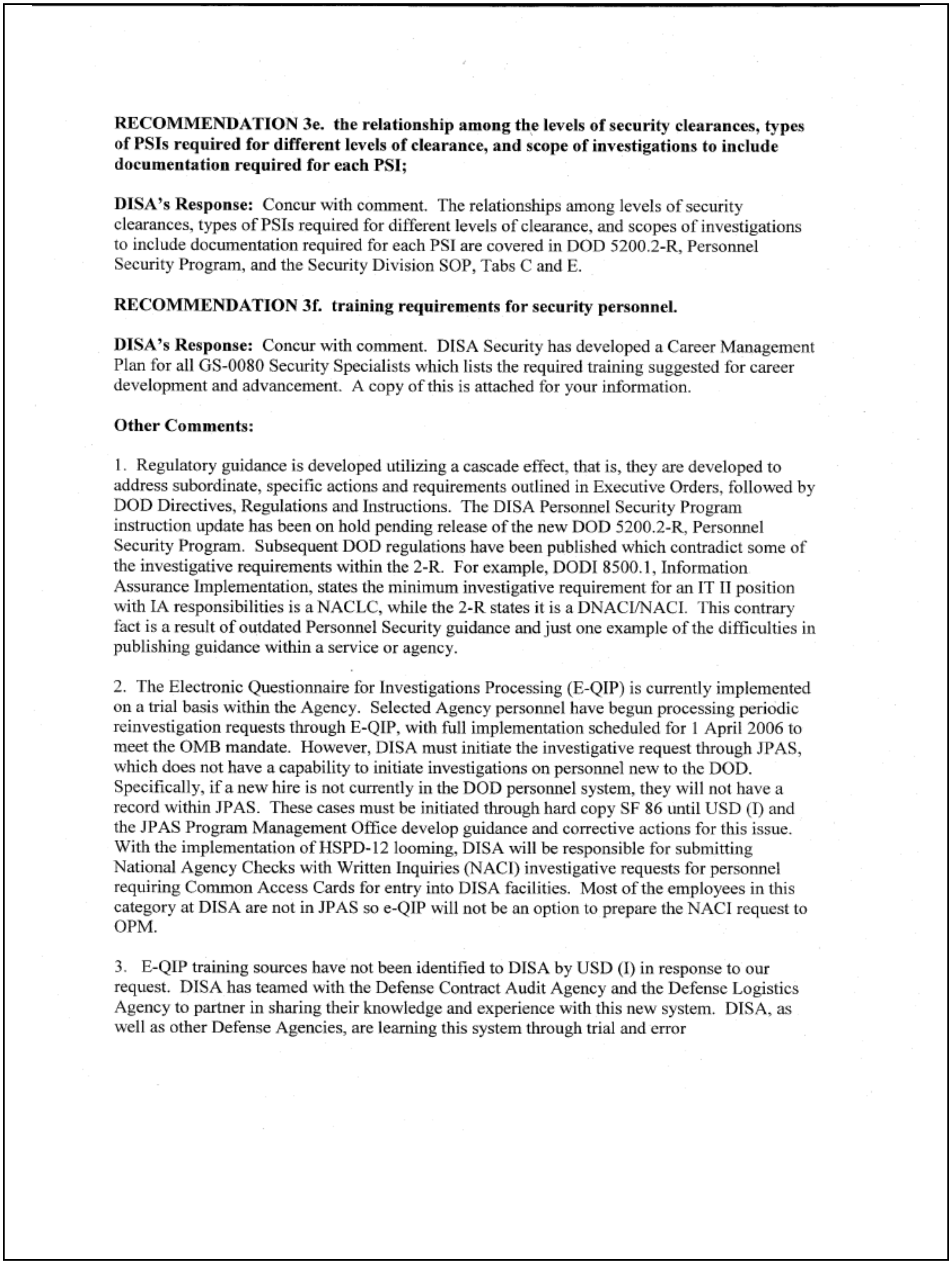
DISA's Response: Concur with comment. The Office of Personnel Management (OPM) is responsible for conducting PSI investigations as identified in your report, and this is addressed in the Personnel Security Standard Operating Procedures, TAB C, paragraph 4.4., that was updated in November 2005.

RECOMMENDATION 3c. security clearance systems for tracking security clearance information;

DISA's Response: Concur. The Joint Personnel Adjudications System (JPAS) has been addressed in previous Security Director Policy Letters and has been incorporated into the draft Instruction as the sole clearance verification system for DOD. Estimated completion date is 15 May 2006.

RECOMMENDATION 3d. PSI submission process.

DISA's Response: Concur with comment. The PSI submission process is addressed in depth in the Security Division Standard Operating Procedures, TAB C that was updated in November 2005.



RECOMMENDATION 3e. the relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scope of investigations to include documentation required for each PSI;

DISA's Response: Concur with comment. The relationships among levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI are covered in DOD 5200.2-R, Personnel Security Program, and the Security Division SOP, Tabs C and E.

RECOMMENDATION 3f. training requirements for security personnel.

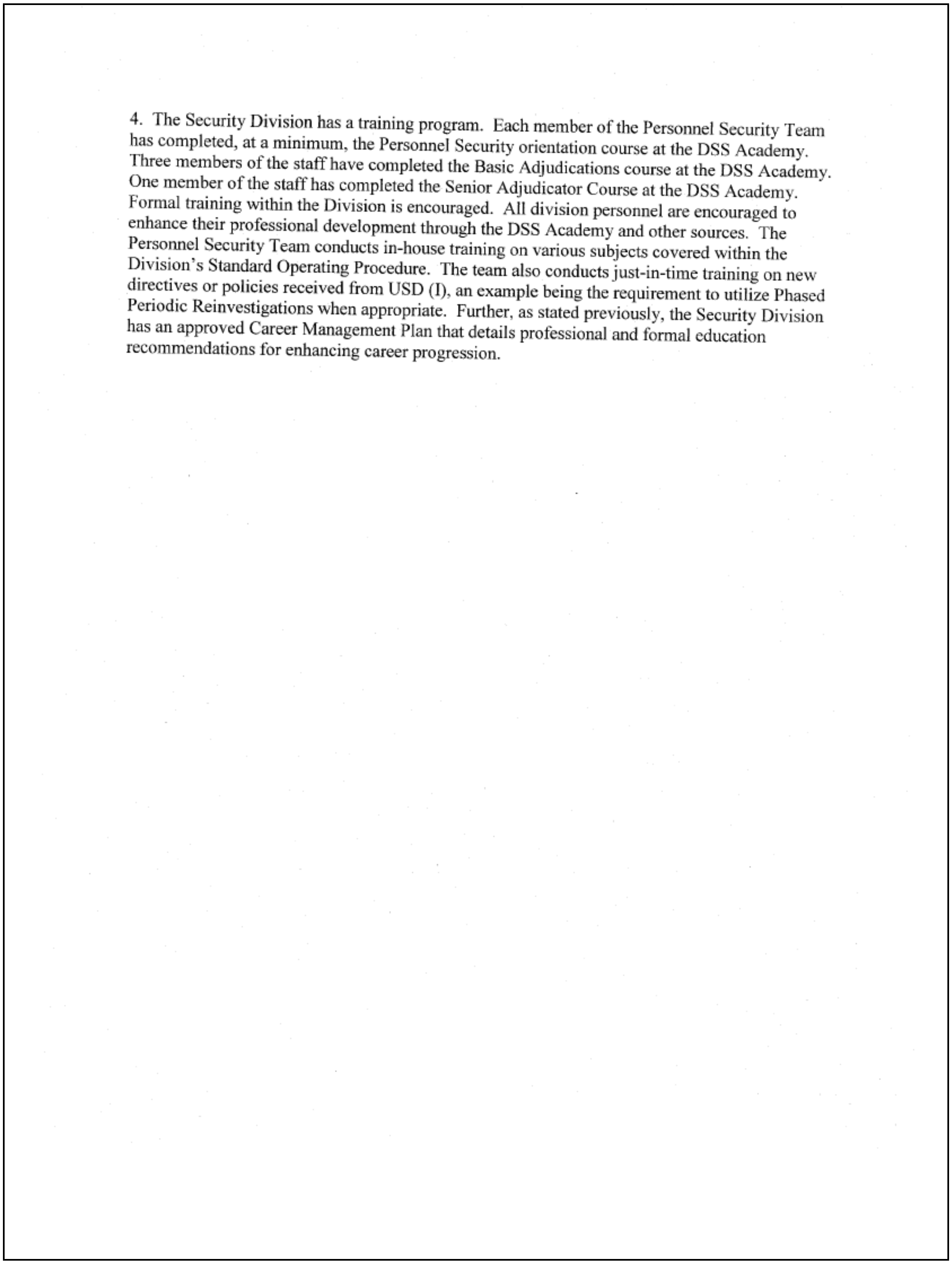
DISA's Response: Concur with comment. DISA Security has developed a Career Management Plan for all GS-0080 Security Specialists which lists the required training suggested for career development and advancement. A copy of this is attached for your information.

Other Comments:

1. Regulatory guidance is developed utilizing a cascade effect, that is, they are developed to address subordinate, specific actions and requirements outlined in Executive Orders, followed by DOD Directives, Regulations and Instructions. The DISA Personnel Security Program instruction update has been on hold pending release of the new DOD 5200.2-R, Personnel Security Program. Subsequent DOD regulations have been published which contradict some of the investigative requirements within the 2-R. For example, DODI 8500.1, Information Assurance Implementation, states the minimum investigative requirement for an IT II position with IA responsibilities is a NACLC, while the 2-R states it is a DNACI/NACI. This contrary fact is a result of outdated Personnel Security guidance and just one example of the difficulties in publishing guidance within a service or agency.

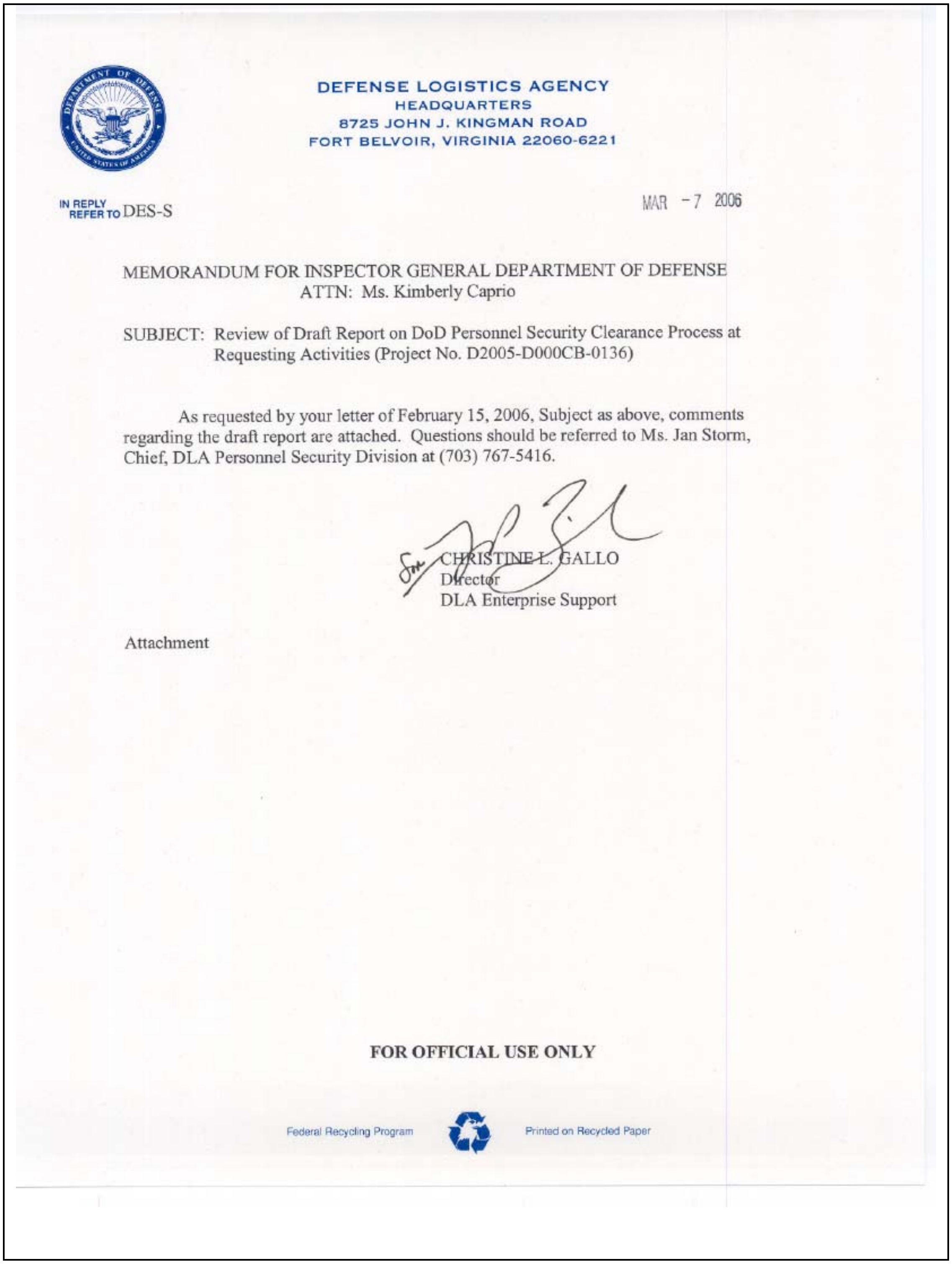
2. The Electronic Questionnaire for Investigations Processing (E-QIP) is currently implemented on a trial basis within the Agency. Selected Agency personnel have begun processing periodic reinvestigation requests through E-QIP, with full implementation scheduled for 1 April 2006 to meet the OMB mandate. However, DISA must initiate the investigative request through JPAS, which does not have a capability to initiate investigations on personnel new to the DOD. Specifically, if a new hire is not currently in the DOD personnel system, they will not have a record within JPAS. These cases must be initiated through hard copy SF 86 until USD (I) and the JPAS Program Management Office develop guidance and corrective actions for this issue. With the implementation of HSPD-12 looming, DISA will be responsible for submitting National Agency Checks with Written Inquiries (NACI) investigative requests for personnel requiring Common Access Cards for entry into DISA facilities. Most of the employees in this category at DISA are not in JPAS so e-QIP will not be an option to prepare the NACI request to OPM.

3. E-QIP training sources have not been identified to DISA by USD (I) in response to our request. DISA has teamed with the Defense Contract Audit Agency and the Defense Logistics Agency to partner in sharing their knowledge and experience with this new system. DISA, as well as other Defense Agencies, are learning this system through trial and error



4. The Security Division has a training program. Each member of the Personnel Security Team has completed, at a minimum, the Personnel Security orientation course at the DSS Academy. Three members of the staff have completed the Basic Adjudications course at the DSS Academy. One member of the staff has completed the Senior Adjudicator Course at the DSS Academy. Formal training within the Division is encouraged. All division personnel are encouraged to enhance their professional development through the DSS Academy and other sources. The Personnel Security Team conducts in-house training on various subjects covered within the Division's Standard Operating Procedure. The team also conducts just-in-time training on new directives or policies received from USD (I), an example being the requirement to utilize Phased Periodic Reinvestigations when appropriate. Further, as stated previously, the Security Division has an approved Career Management Plan that details professional and formal education recommendations for enhancing career progression.

Defense Logistics Agency Comments



DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO DES-S

MAR -7 2006

MEMORANDUM FOR INSPECTOR GENERAL DEPARTMENT OF DEFENSE
ATTN: Ms. Kimberly Caprio

SUBJECT: Review of Draft Report on DoD Personnel Security Clearance Process at Requesting Activities (Project No. D2005-D000CB-0136)

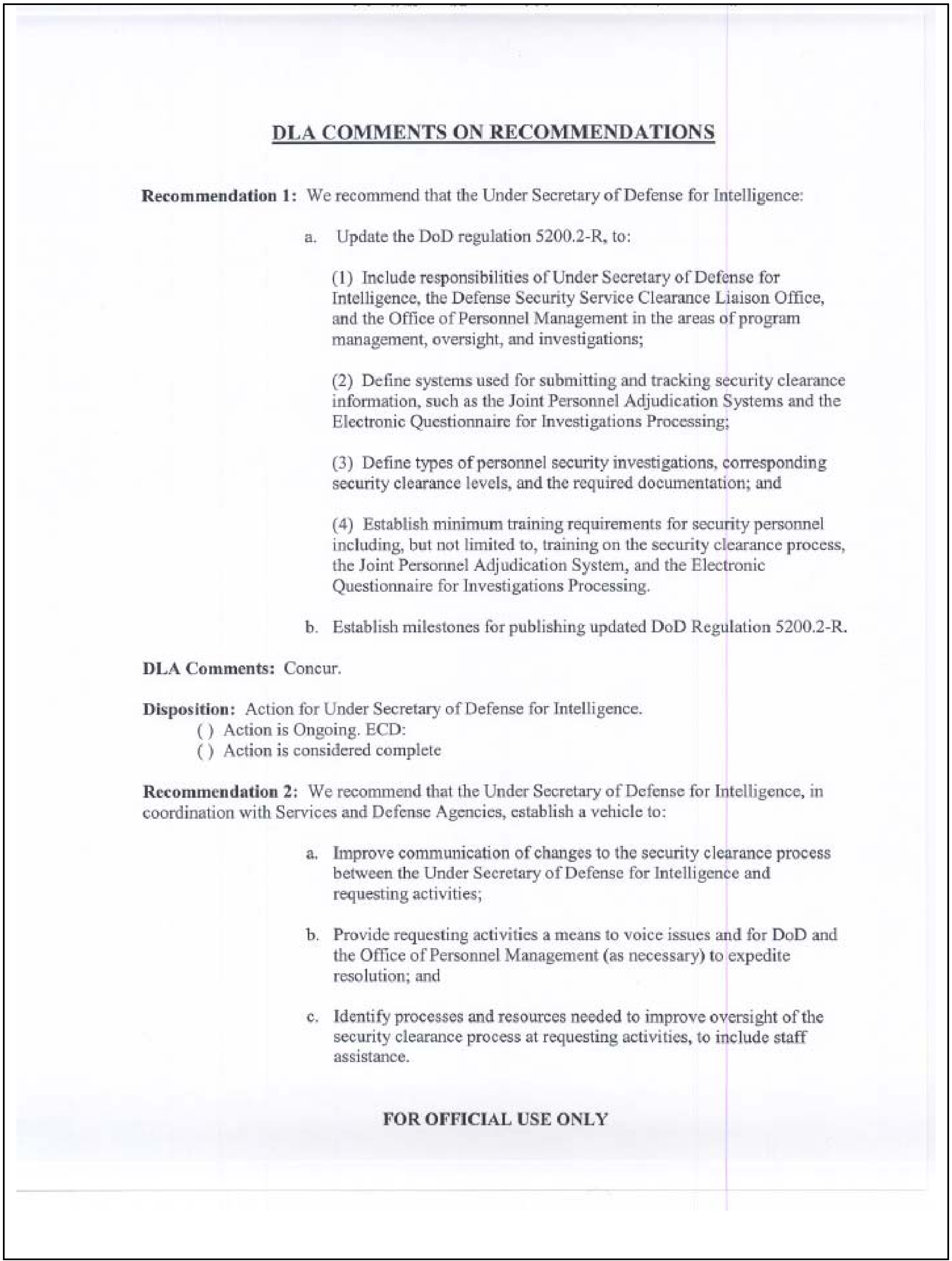
As requested by your letter of February 15, 2006, Subject as above, comments regarding the draft report are attached. Questions should be referred to Ms. Jan Storm, Chief, DLA Personnel Security Division at (703) 767-5416.

CHRISTINE L. GALLO
Director
DLA Enterprise Support

Attachment

FOR OFFICIAL USE ONLY

Federal Recycling Program Printed on Recycled Paper



DLA COMMENTS ON RECOMMENDATIONS

Recommendation 1: We recommend that the Under Secretary of Defense for Intelligence:

a. Update the DoD regulation 5200.2-R, to:

(1) Include responsibilities of Under Secretary of Defense for Intelligence, the Defense Security Service Clearance Liaison Office, and the Office of Personnel Management in the areas of program management, oversight, and investigations;

(2) Define systems used for submitting and tracking security clearance information, such as the Joint Personnel Adjudication Systems and the Electronic Questionnaire for Investigations Processing;

(3) Define types of personnel security investigations, corresponding security clearance levels, and the required documentation; and

(4) Establish minimum training requirements for security personnel including, but not limited to, training on the security clearance process, the Joint Personnel Adjudication System, and the Electronic Questionnaire for Investigations Processing.

b. Establish milestones for publishing updated DoD Regulation 5200.2-R.

DLA Comments: Concur.

Disposition: Action for Under Secretary of Defense for Intelligence.
( ) Action is Ongoing. ECD:
( ) Action is considered complete

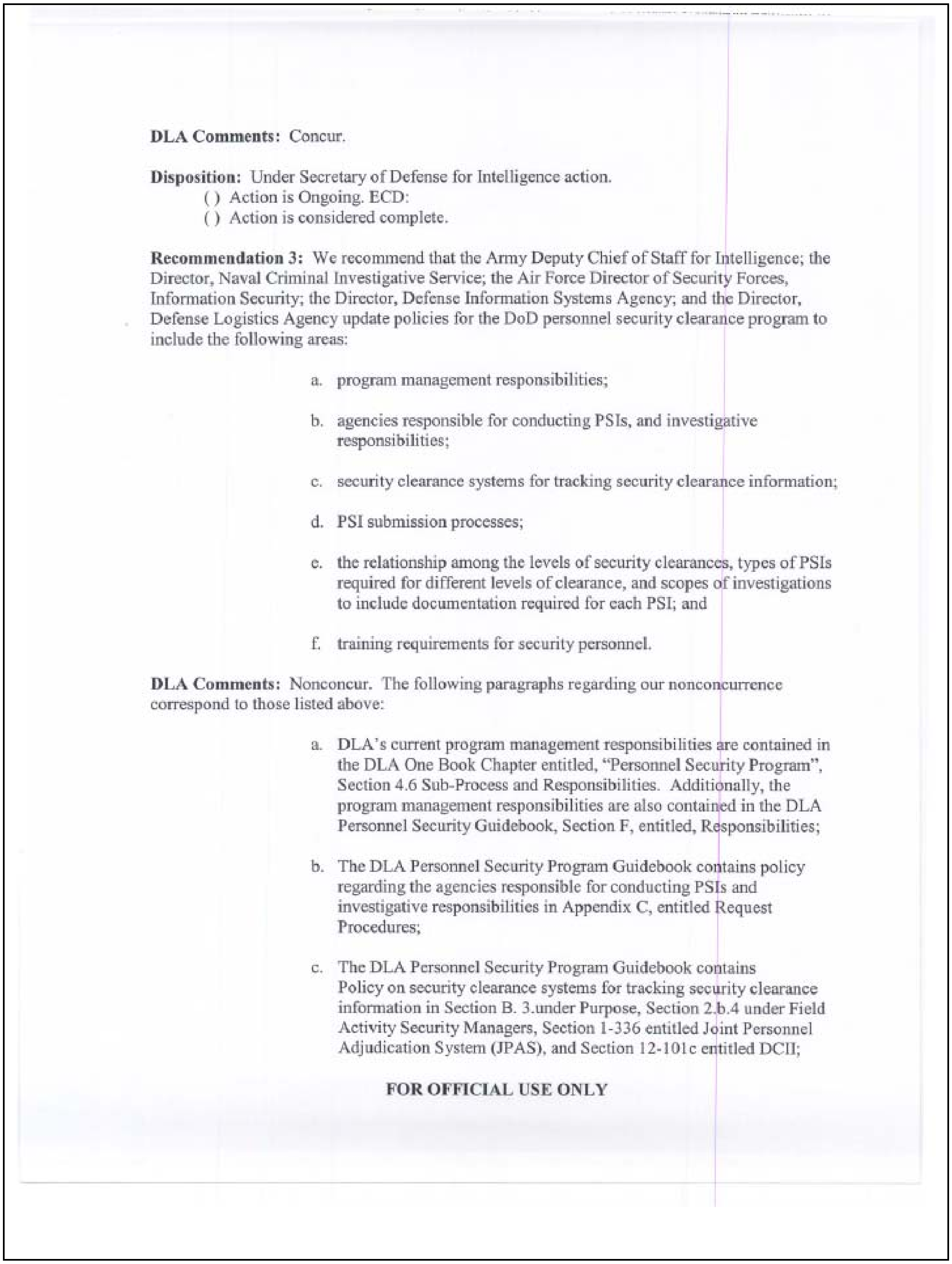
Recommendation 2: We recommend that the Under Secretary of Defense for Intelligence, in coordination with Services and Defense Agencies, establish a vehicle to:

a. Improve communication of changes to the security clearance process between the Under Secretary of Defense for Intelligence and requesting activities;

b. Provide requesting activities a means to voice issues and for DoD and the Office of Personnel Management (as necessary) to expedite resolution; and

c. Identify processes and resources needed to improve oversight of the security clearance process at requesting activities, to include staff assistance.

FOR OFFICIAL USE ONLY



DLA Comments: Concur.

Disposition: Under Secretary of Defense for Intelligence action.
( ) Action is Ongoing. ECD:
( ) Action is considered complete.

Recommendation 3: We recommend that the Army Deputy Chief of Staff for Intelligence; the Director, Naval Criminal Investigative Service; the Air Force Director of Security Forces, Information Security; the Director, Defense Information Systems Agency; and the Director, Defense Logistics Agency update policies for the DoD personnel security clearance program to include the following areas:

a. program management responsibilities;

b. agencies responsible for conducting PSIs, and investigative responsibilities;

c. security clearance systems for tracking security clearance information;

d. PSI submission processes;

e. the relationship among the levels of security clearances, types of PSIs required for different levels of clearance, and scopes of investigations to include documentation required for each PSI; and

f. training requirements for security personnel.

DLA Comments: Nonconcur. The following paragraphs regarding our nonconcurrence correspond to those listed above:

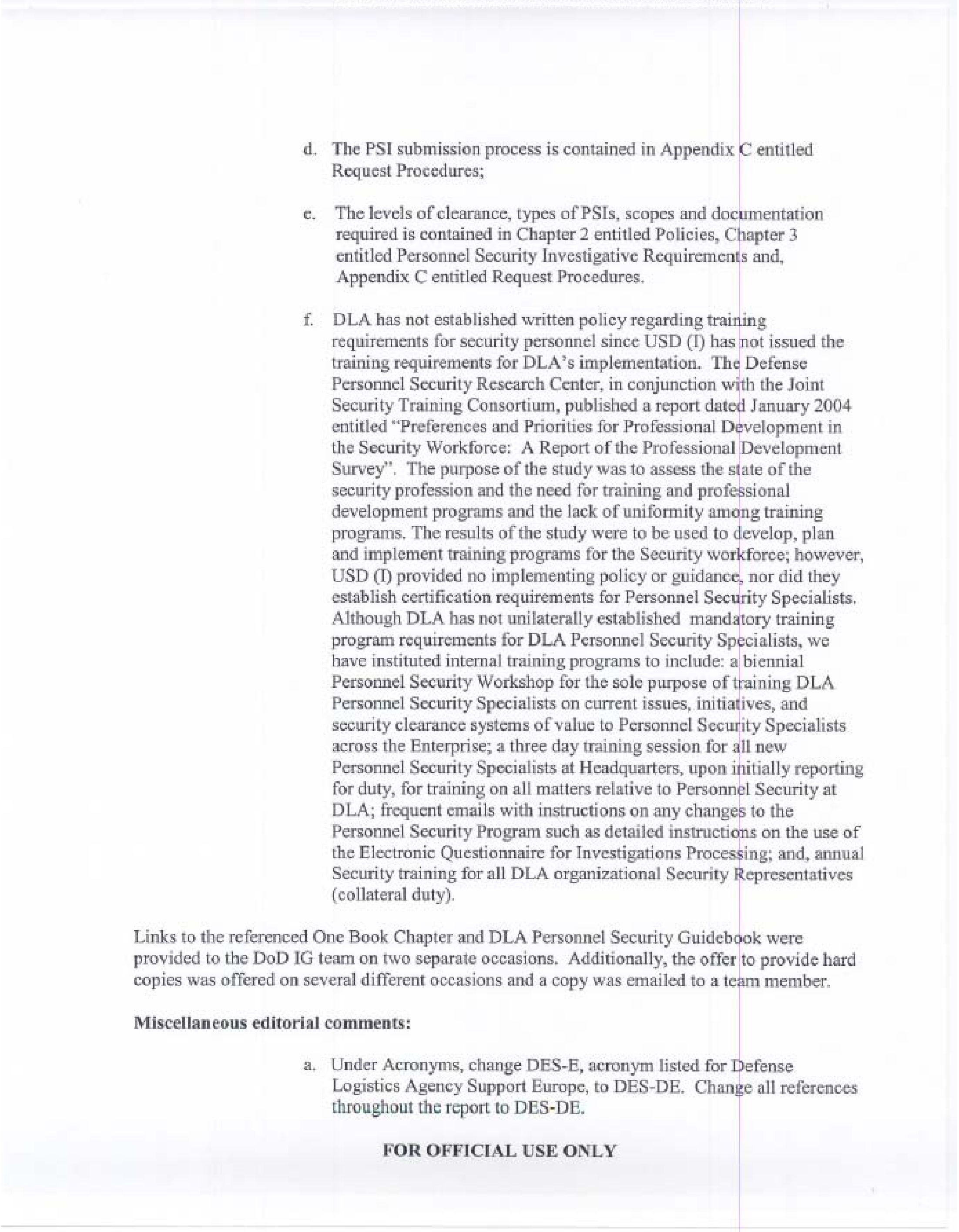
a. DLA's current program management responsibilities are contained in the DLA One Book Chapter entitled, "Personnel Security Program", Section 4.6 Sub-Process and Responsibilities. Additionally, the program management responsibilities are also contained in the DLA Personnel Security Guidebook, Section F, entitled, Responsibilities;

b. The DLA Personnel Security Program Guidebook contains policy regarding the agencies responsible for conducting PSIs and investigative responsibilities in Appendix C, entitled Request Procedures;

c. The DLA Personnel Security Program Guidebook contains Policy on security clearance systems for tracking security clearance information in Section B. 3.under Purpose, Section 2.b.4 under Field Activity Security Managers, Section 1-336 entitled Joint Personnel Adjudication System (JPAS), and Section 12-101c entitled DCII;

FOR OFFICIAL USE ONLY

Final Report Reference



d. The PSI submission process is contained in Appendix C entitled Request Procedures;

e. The levels of clearance, types of PSIs, scopes and documentation required is contained in Chapter 2 entitled Policies, Chapter 3 entitled Personnel Security Investigative Requirements and, Appendix C entitled Request Procedures.

f. DLA has not established written policy regarding training requirements for security personnel since USD (I) has not issued the training requirements for DLA's implementation. The Defense Personnel Security Research Center, in conjunction with the Joint Security Training Consortium, published a report dated January 2004 entitled "Preferences and Priorities for Professional Development in the Security Workforce: A Report of the Professional Development Survey". The purpose of the study was to assess the state of the security profession and the need for training and professional development programs and the lack of uniformity among training programs. The results of the study were to be used to develop, plan and implement training programs for the Security workforce; however, USD (I) provided no implementing policy or guidance, nor did they establish certification requirements for Personnel Security Specialists. Although DLA has not unilaterally established mandatory training program requirements for DLA Personnel Security Specialists, we have instituted internal training programs to include: a biennial Personnel Security Workshop for the sole purpose of training DLA Personnel Security Specialists on current issues, initiatives, and security clearance systems of value to Personnel Security Specialists across the Enterprise; a three day training session for all new Personnel Security Specialists at Headquarters, upon initially reporting for duty, for training on all matters relative to Personnel Security at DLA; frequent emails with instructions on any changes to the Personnel Security Program such as detailed instructions on the use of the Electronic Questionnaire for Investigations Processing; and, annual Security training for all DLA organizational Security Representatives (collateral duty).

Links to the referenced One Book Chapter and DLA Personnel Security Guidebook were provided to the DoD IG team on two separate occasions. Additionally, the offer to provide hard copies was offered on several different occasions and a copy was emailed to a team member.

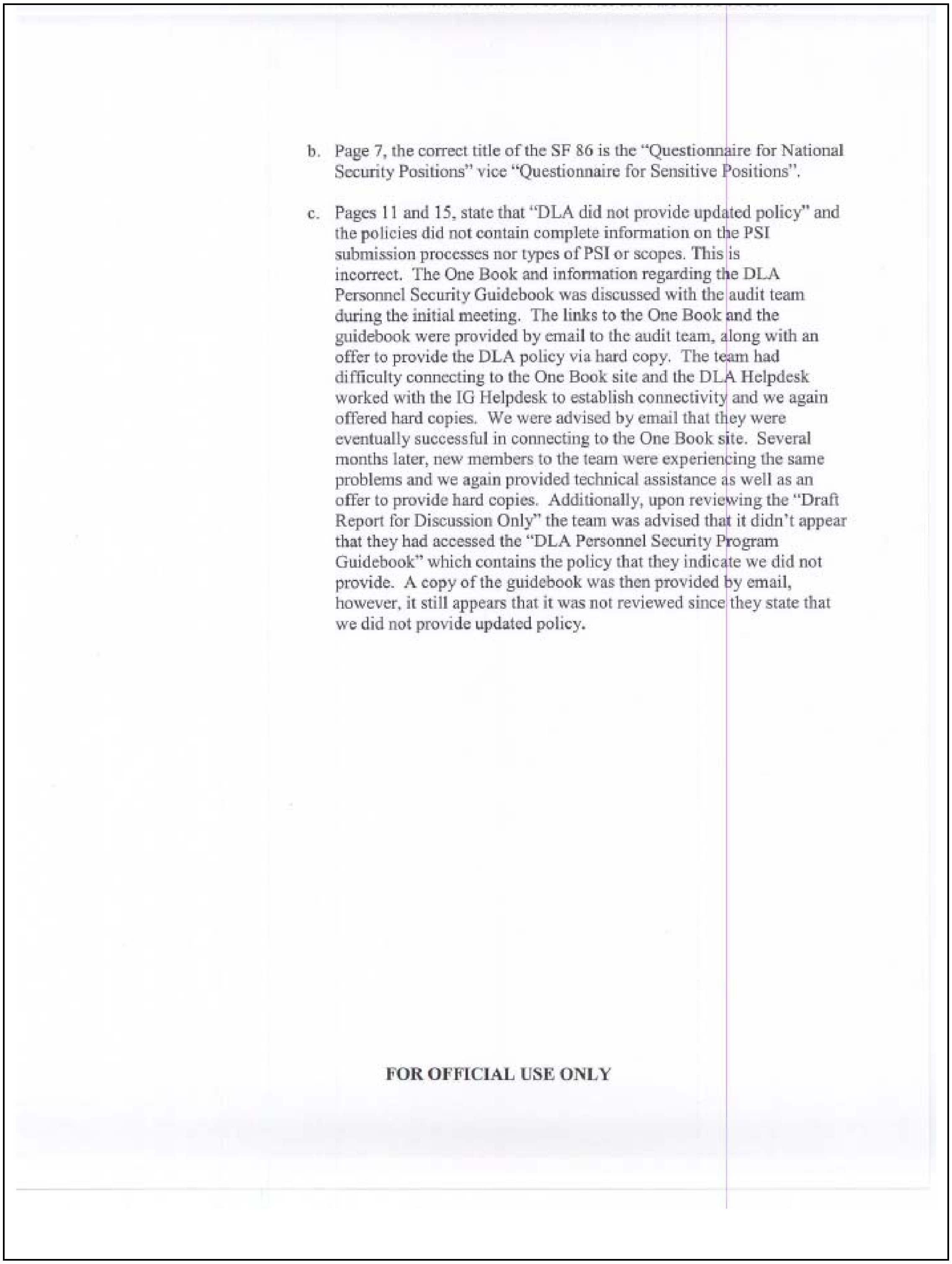
Miscellaneous editorial comments:

Revised

a. Under Acronyms, change DES-E, acronym listed for Defense Logistics Agency Support Europe, to DES-DE. Change all references throughout the report to DES-DE.

FOR OFFICIAL USE ONLY

Final Report Reference



b. Page 7, the correct title of the SF 86 is the "Questionnaire for National Security Positions" vice "Questionnaire for Sensitive Positions".

Revised

c. Pages 11 and 15, state that "DLA did not provide updated policy" and the policies did not contain complete information on the PSI submission processes nor types of PSI or scopes. This is incorrect. The One Book and information regarding the DLA Personnel Security Guidebook was discussed with the audit team during the initial meeting. The links to the One Book and the guidebook were provided by email to the audit team, along with an offer to provide the DLA policy via hard copy. The team had difficulty connecting to the One Book site and the DLA Helpdesk worked with the IG Helpdesk to establish connectivity and we again offered hard copies. We were advised by email that they were eventually successful in connecting to the One Book site. Several months later, new members to the team were experiencing the same problems and we again provided technical assistance as well as an offer to provide hard copies. Additionally, upon reviewing the "Draft Report for Discussion Only" the team was advised that it didn't appear that they had accessed the "DLA Personnel Security Program Guidebook" which contains the policy that they indicate we did not provide. A copy of the guidebook was then provided by email, however, it still appears that it was not reviewed since they state that we did not provide updated policy.

Revised

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Acquisition and Contract management prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Richard B. Jolliffe
Kimberley A. Caprio
Riccardo R. Buglisi
Carol N. Gorman
Melissa M. McBride
Susan R. Ryan
Shantiki S. Sanders
Rachel M. Miller
Antwan M. Jackson
Jillisa H. Milner