Audit Report

DEFENSE CLEARANCE AND INVESTIGATIONS
INDEX DATABASE

Report No. D-2001-136 June 7, 2001

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

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

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

Defense Hotline

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

Acronyms

ASD (C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CAF	Central Adjudication Facility
DCII	Defense Clearance and Investigations Index
DMDC	Defense Manpower Data Center
DSS	Defense Security Service
DSSOC-C	Defense Security Service Operation Center-Columbus
LAA	Limited Access Authority
NRO	National Reconnaissance Office
OPM	Office of Personnel Management
PMO	Program Management Office
SSN	Social Security Number

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

June 7, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Audit Report on the Defense Clearance and Investigations Index Database (Report No. D-2001-136)

We are providing this report for review and comment. The Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director, Defense Security Service, did not respond to the draft.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We request that the Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director, Defense Security Service, provide comments on the recommendations by July 9, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil) or Ms. Judith I. Padgett at (703) 604-8990 (DSN 664-8990) (jpadgett@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-136 **June 7, 2001**
(Project No. D2000AD-0132)

Defense Clearance and Investigations Index Database

Executive Summary

Introduction. The Department of Defense established the Defense Clearance and Investigations Index (DCII) in 1967 as the single, automated central repository that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities. The Deputy Assistant Secretary for Defense, Security and Information Operations, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is responsible for providing policy and guidance for the DCII. The Defense Security Service is the executive agency responsible for maintaining system hardware and applications for storage and retrieval of data in the DCII. The DoD investigative agencies and central adjudicative facilities are responsible for the accuracy of data entered in the DCII. As of March 2000, the DCII had approximately 24 million individuals indexed, with approximately 30 million investigative dossiers and security clearance eligibility tracings.

Objectives. The overall audit objective was to determine the accuracy, integrity, timeliness, and availability of information in the DCII database. The audit determined the impact of DCII information on the future Joint Personnel Adjudication System.

Results. An estimated 1.4 million of the 24 million DoD personnel, contractors, and foreign nationals in the DCII had incomplete social security number-based investigative dossiers and clearance tracings. The Army Crime Records Division and the Navy Criminal Investigative Service reported a cumulative estimate of over 107,000 obsolete investigative dossiers and clearance tracings in the DCII. Data reliability affected the productivity of DoD adjudicators and security officers, and impeded reasonably estimating the number of periodic reinvestigations needed (finding A).

The Defense Security Service Operation Center-Columbus assigned over 1,400 pseudo social security numbers of which 524 were inconsistent and did not conform to Office of Personnel Management guidance. In addition, no tracking process was established for foreign nationals with limited access authority and indexed in the Defense Clearance and Investigations Index. As a result, foreign nationals were inadequately identified in the DCII, and multiple foreign nationals were assigned the same pseudo social security number (finding B).

Summary of Recommendations. We recommend that the Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) establish a unique primary personal identifier to enter data in the DCII; establish quarterly analysis of the DCII for obsolete records; and revise guidance regarding pseudo social security numbers.

We recommend that the Director, Defense Security Service, modify the Defense Clearance and Investigations Index to restore functions and validate social security number fields. We further recommend that the Director establish procedures to compare and update operations and regulatory documents, incorporate Federal guidelines, and identify and delete test data.

Management Comments. We issued a draft of this report February 15, 2001. We did not receive comments from the Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), and the Director, Defense Security Service, and request that they provide comments by July 9, 2001.

Although not required to comment, the Naval Criminal Investigative Service provided comments on the audit results and recommendations. The Naval Criminal Investigative Service generally agreed with the recommendations except for the recommendation to establish the social security number as a unique identifier. We discuss the Naval Criminal Investigative Service comments on the recommendations following each applicable recommendation. A discussion of the comments on the audit results is in Appendix D of the report and the complete text is in the Management Comments section.

Table of Contents

Executive Summary

Introduction

Background 1
Objectives 2

Findings

A. Integrity of Data in the Defense Clearance and Investigations Index Database 3
B. Pseudo Social Security Numbers for Foreign Nationals 13

Appendixes

A. Audit Process
Scope and Methodology 18
Management Control Program Review 19
B. Prior Coverage 20
C. Defense Clearance and Investigations Index Contributors and Non-Department of Defense Users 21
D. Audit Response to Naval Criminal Investigative Service Comments Concerning the Report 23
E. Report Distribution 24

Management Comments

Naval Criminal Investigative Service 27

Background

Defense Clearance and Investigations Index. In 1967, DoD established the Defense Clearance and Investigations Index (DCII) as the single, automated central repository that identifies investigations conducted by DoD investigative agencies. In 1977, the DCII was expanded to index personnel security determinations made by DoD adjudicative authorities. The Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C^3I]) establishes policy and guidance for maintenance of and access to the DCII. The guidance is included in DoD Regulation 5200.2-R, "Personnel Security Program," January 1987.

The Defense Security Service (DSS) is the executive agency responsible for maintaining the hardware and system applications that allow DCII contributors and users to enter, access, and retrieve data in the DCII. However, except for data on opened and closed personnel security investigations entered by the Personnel Investigations Center, the data in the DCII is not owned by DSS. The various contributors that enter data in the DCII are responsible for ensuring data accuracy and currency.

Fifteen DoD organizations enter criminal and security investigative results and personnel security clearance adjudicative decisions in the DCII. Nine non-DoD organizations have limited access to the DCII to review criminal and personnel security investigative results and personnel security clearance eligibility and access. See Appendix C for a list of the major DCII contributors and non-DoD users that have access to the database.

Case Control Management System. The Case Control Management System is the centerpiece of the overall DSS Corporate Enterprise System. It guides and controls the hardware and software application for opening, tracking, and closing personnel investigation cases. The Corporate Enterprise System is a combination of 24 primary information systems, subsystems, applications, and interfaces that share common data that is stored in the central corporate database and linked by Case Control Management System. The Case Control Management System receives, stores, and acts upon personnel security requests, such as personnel security updates and requests for investigation. The Case Control Management System automated case workflow process feeds information through several interfaces and then to final storage in the central corporate database. The status of personnel security investigations and periodic reinvestigations for individuals indexed with security clearance eligibility and access is tracked in the Case Control Management System and stored in the central corporate database. That central corporate database includes the DCII and can be accessed by DCII contributors and users to retrieve investigative and security clearance information from individuals' records.

Objectives

The overall objective was to determine the accuracy, integrity, timeliness, and availability of information in the DCII database. The audit determined the impact of DCII information on the future Joint Personnel Adjudication System. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for prior coverage related to the audit objectives.

DCII Effect on the Joint Personnel Adjudication System

The DCII does not affect the Joint Personnel Adjudication System. The Joint Personnel Adjudication System is the DoD personnel security system being developed for the DoD central adjudication facilities (CAFs), DoD security managers, and special security officers. The Joint Personnel Adjudication System will store security clearance information on DoD military, civilian, and contractor personnel; however, it will not replace the DCII because it will not store criminal and personnel security investigative data. When fully implemented in FY 2002, the Joint Personnel Adjudication System will represent the virtual consolidation of the DoD CAFs and will ensure standardization and re-engineering of core personnel security and adjudication processes. The Joint Personnel Adjudication System will use a common database with centralized computer hardware and software application programs that will not be affected by DCII information. The DCII will still be populated with DoD military, civilian, and contractor personnel security clearances to facilitate reciprocity with non-DoD organizations.

A. Integrity of Data in the Defense Clearance and Investigations Index Database

An estimated 1.4 million of the 24 million DoD personnel, contractors, and foreign nationals in the DCII had incomplete social security number-based investigative dossiers and clearance tracings. The Army Crime Records Division and the Navy Criminal Investigative Service reported a cumulative estimate of over 107,000 obsolete investigative dossiers and clearance tracings in the DCII. The data integrity of the DCII was impaired because specific controls and procedures were not established. As a result, DCII data reliability affected the productivity of DoD adjudicators and security officers. Also, DCII data reliability could continue to impede the Defense agencies' ability to reasonably estimate the number of periodic reinvestigations needed.

DoD Guidance Establishing Requirements for Data in the DCII

DoD Regulation 5200.2-R, "Personnel Security Program" January 1987, Chapter XII*, establishes requirements for indexing investigative and adjudicative data in the DCII. The DCII investigative data consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects named in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative organizations. The DCII also includes security adjudicative determinations on DoD personnel and contractors by subject.

Investigative Data. DoD Regulation 5200.2-R states that all investigative data on an individual must include the following:

- indicate the opening of a pending investigation;
- reflect a completed investigation, including the date (year) of the investigation; and
- reflect changes or additions, whenever appropriate.

The Regulation further states that investigative file tracings may be deleted from the DCII when the retention period is over and the record file has been destroyed.

* Chapter XII was added by change 3, February 23, 1996.

Adjudicative Data. DoD Regulation 5200.2-R requires that all adjudicative determinations on personnel with access to classified information or performing sensitive duties be indexed in the DCII. Specifically, the Regulation states that creating or updating a DCII clearance tracing is required:

- immediately upon suspension of access;
- following authorization of an interim access by the CAF or employing organization;
- immediately following granting, denying, or revoking a clearance or access; and
- following the receipt, review, and adjudication of information received subsequent to an earlier clearance or access determination.

The Regulation also states that an adjudicative determination shall remain in the DCII as long as the subject is affiliated with the DoD. The determination may be deleted 2 years after either the subject's employment or clearance eligibility ends. The deleted DCII data shall be retained by DSS in a historical file for a minimum of 5 years after deletion by the contributor. The Regulation requires that the date of the DCII security clearance eligibility determination or access entry shall always be the same as or subsequent to the date of the most recent personnel security investigation. The Regulation further requires that DoD Components notify the CAF of applicable personnel changes to ensure the accuracy of the DCII database.

Data Accuracy and Reliability in the DCII

Accuracy of Mandatory Personal Identifier. Approximately 1.4 million of the approximately 24 million individuals in the DCII, as of March 2000, were indexed with investigative dossiers and clearance tracings but without a social security number (SSN). DoD grants security clearances to an individual only after extensive background investigation and review of the investigative results to determine an individual's loyalty to the United States, trustworthiness, and integrity. To ensure positive identification of the subject of a personal security investigation, investigators use the individual's SSN to obtain and review pertinent documents. The investigative results are provided to the DoD adjudication facilities to review and determine whether the individual meets the criteria for a security clearance. Throughout the investigative and adjudicative process, an individual's SSN is used for identification. To have individuals indexed with security clearance eligibility and access in the DCII without an SSN is a data anomaly.

The DCII User's Manual states the system requirement for the name and one other personal identifier field for entering DCII data. The other personal identifier choices, in addition to the name entry, were the person's SSN, date of birth, or place of birth.

Using a person's name does not create a unique identifier in the same way that an SSN would, and the DCII had no means to check for possible duplications based on name variations. For example, if investigators or adjudicators entered information about Jane E. Smith, each using a variation of her name, multiple individual records would be created (Jayne E. Smith, Janie Smith, Jane Smith). Misspellings, even punctuation differences, caused the system to create a new record if one of the other three fields also had data entered in it.

A Defense Manpower Data Center (DMDC) analysis of the clearance tracings portion of the DCII, as of December 31, 1999, showed that 2,394 individuals with clearance tracings had no SSN recorded in DCII. Further analysis showed that 89 of the 2,394 individuals had an SSN recorded in other DoD personnel databases. The 89 individuals in the analysis were identified by using the individual's name, date of birth, and place of birth recorded in the DCII and matching that information to records in DoD Active and Reserve military, civilian, and nonappropriated fund personnel databases as of September 2000.

We believe that use of the SSN data field as the mandatory personal identifier field would significantly reduce the likelihood of multiple entries and erroneous matches in the DCII because variations are not commonly made on numbers as they are on names. Requiring the use of a valid SSN or an approved personnel identification number in the SSN data field would also facilitate adjudicators' efforts to retrieve and review all DCII records for individuals being reviewed for security clearance eligibility and access.

Reliability of Personal Identifier. Criminal investigators used invalid SSNs to index subjects of a criminal investigation in the DCII and the investigators assigned the same SSN to several of the subjects indexed. DoD Instruction 5505.7, "Titling and Indexing of Subjects of Criminal Investigations in the Department of Defense," May 14, 1992, states:

> The DoD standard that shall be applied when titling and indexing the subjects of criminal investigations is a determination that credible information exists that a person or entity may have committed a criminal offense or is otherwise made the object of a criminal investigation.

The Instruction further states that the investigative agency shall report the identity of the subject when known at the start of the investigation and in accordance with DCII procedures. When criminal investigators index subjects of criminal investigations in the DCII without the subject's valid SSN, DoD adjudicators could potentially miss information relating to the trustworthiness and integrity of those individuals when making adjudicative determinations. Also, security officers may inappropriately validate hiring or grant access to classified information to individuals who were improperly indexed in the DCII.

Criminal investigators used invalid SSNs because they believed that a 9-digit number was required in the SSN data field. The Army Crime Records Division and the Air Force Office of Special Investigation--offices that had entered several invalid SSNs--stated that those invalid SSNs were entered to fill the field when they did not have a person's SSN. During the audit, personnel at Army

Crime Records Division were instructed to no longer enter a fictitious 9-digit number in the SSN data field when the SSN is not known.

A DMDC analysis of the clearance-tracing portion of the DCII, as of December 31, 1999, showed that 6,323 individuals indexed with clearance tracings had invalid SSNs recorded in the DCII. DMDC used the Social Security Administration guidelines for identifying valid and invalid SSNs in analyzing the DCII data. Further analysis using the September 2000 DMDC database for DoD Active and Reserve military, civilian, and nonappropriated fund personnel showed that at least 1,402 individuals with invalid SSNs in DCII could be matched to valid SSNs in other systems.

Reliability of Country Code Data. Some clearance tracings that DoD CAF personnel entered did not process during batch transmission because of inconsistent country codes recorded in the individuals' country-of-birth data field. The DoD CAF personnel expressed concern regarding country codes used in the DCII database.

DSS personnel stated that they use the Federal Information Processing Standard Publication (FIPS PUB 10-4), "Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions" as the source for country codes. The DCII User's Manual lists the country codes that CAF personnel should use. Changes to that list must be approved by the Director, Security Programs, ASD(C^3I).

FIPS PUB 10-4 is the Federal Government's standardized list of geopolitical information retrieval codes for the State Department and national defense programs, as well as other Federal and non-Federal organizations. Analysis of the DCII User's Manual showed that the Manual included the following:

- 263 country codes compared to 262 listed in the FIBS PUB 10-4;
- 20 country codes not in the FIPS PUB 10-4; and
- 14 country codes missing that were in the FIPS PUB 10-4.

User Needs for DCII Capabilities

When DSS transferred data processing to the Corporate Enterprise System, the DCII lost functions to mass delete investigative dossiers and clearance tracings and the ability to transmit NRO investigative and adjudicative data in batches. According to DCII system Problems and Change Requests reports, DCII users requested that the Information Technology PMO implement those functions and other modifications in the DCII. In addition, in August 1997, the DCII Users Council requested that DSS modify the DCII to allow its contributors to enter supplemental adjudicative information in a dossier line. The requests were not met as of October 2000. Major system problems with the Case Control Management System resulted in the Information Technology PMO programming effort on the Case Control Management System receiving higher priority compared to the DCII system Problems and Change Requests. Delay in

implementing the mass deletion and the batch transmission functions, along with other changes requested, contributed to inaccurate, unreliable, and obsolete data in the DCII. The lost functions and requested modifications are discussed below.

Processing Functions Needed in the DCII. The processing functions that DCII contributors and users wanted reestablished fell into two categories. First, DCII contributors and users wanted to reestablish a function that would allow DSS to mass delete obsolete investigative dossiers and clearance tracings in the DCII. Second, NRO, a DCII contributor and user, wanted to reestablish a function that would transmit batches of data.

Mass Deletion of Obsolete Dossiers and Clearance Tracings. With the transfer of data processing to the Corporate Enterprise System, DSS lost the function in the DCII to mass delete obsolete investigative dossiers and clearance tracings. DoD Regulation 5200.2-R states that investigative data may be deleted from the DCII when the retention period is over and the record has been destroyed. The Regulation also states that adjudicative determinations may be deleted 2 years after either the individual's employment or clearance eligibility ends.

The Army Crime Records Division and the Navy Criminal Investigation Service identified dossiers for individuals that could be deleted from the DCII because the retention periods had passed. Personnel at the Army Crime Records Division estimated that they could delete 64,335 investigative dossiers from the DCII. Personnel at the Navy Criminal Investigative Service deleted 18,759 investigative dossiers and tracings from the DCII manually. The Navy Criminal Investigative Service estimated that it still needed to delete more than 43,000 dossiers and tracings for the closed cases they sent to the Federal Records Center in July 1999. Personnel at the Navy Criminal Investigative Service were waiting for DSS to provide a list of aged dossiers and tracings so they could authorize DSS to mass delete those records.

The Director, Security Programs, ASD(C^3I), established a process to identify records with clearance tracings that could be deleted from the DCII. DSS provided a quarterly tape of DCII records with clearance tracings to DMDC. DMDC analyzed the DCII records and matched those records with records in DoD Active and Reserve military, civilian, and nonappropriated funds personnel databases to identify DCII records that could be purged. DMDC provided a file, sorted using the DCII contributor identification, to the Office of the Director, Security Programs, ASD(C^3I), for distribution to the contributors for review. The DCII contributors approved the records for mass deletion and notified DSS. However, DSS had not used that procedure since 1998.

The DSS transfer of data processing to the Corporate Enterprise System in 1998 caused system application and data integrity problems, including identification of personnel security investigative closing dates in the DCII. To transfer records to the Corporate Enterprise System, DSS recorded the year 1921 in the investigative close date for records of DoD contractor personnel who did not have an investigative date in the clearance tracing.

The Director, Security Programs, ASD (C^3I), had not requested that DMDC provide information on unmatched records found as a result of matching DCII records with records in DoD personnel databases since the transfer of data processing to the Corporate Enterprise System. DMDC had not received any requests for an aging analysis of criminal investigative dossiers to identify dossiers past their retention period. We believe an analysis of those two categories of records could identify additional DCII records that could be purged from the database.

Batch Processing of NRO Data Transmissions. With the transfer of data processing to the Corporate Enterprise System, DSS lost the capability in the DCII for NRO to batch transmit opened and closed personnel security investigations. Although NRO was able to enter its adjudicative actions, the associated investigations upon which those adjudicative decisions were made were not current in the DCII. Since losing the automated batch transmission capability to update personnel security investigative dossiers in the DCII, NRO could only enter investigative dossiers and adjudicative determinations on a small, select group of individuals. In a January 1999 meeting with NRO security personnel, DSS senior management pledged to resolve the issue relating to the NRO data entry of investigative actions in the DCII. As of October 5, 2000, the batch processing function had not been restored, and NRO had approximately 23,000 records that needed updating in the DCII.

In an October 1999 memorandum to DSS management, the Director of Security, NRO, pointed out that mismatches between investigative and adjudicative entries in the DCII were generating confusion and undesired scrutiny within the security community for individuals associated with NRO. The memorandum emphasizes in closing that the requested modifications are critical and, "... impact community reciprocity, DCII data integrity, and program security."

Requested Adjudicative Dossier Line. DSS had not modified the DCII to allow supplemental adjudicative information in the files, as the Chairperson of the DCII Users' Council requested in August 1997. The requested DCII modification would allow the CAFs to record a tracing or dossier line in the DCII to indicate that the CAF obtained supplemental information to support a favorable determination when the investigative case control number in the personnel security investigative dossier shows derogatory information in the case file. The Washington Headquarters Service CAF spearheaded the effort to justify the adjudicative dossier line in the DCII at the May 1997 DCII Users' Council meeting. The Chairperson of the DCII Users' Council and personnel at Washington Headquarters Service received no information indicating that the modification was accomplished or scheduled.

Specific Controls and Procedures for Maintaining Data Integrity

The data integrity of the DCII was impaired because ASD (C^3I), DSS, and DCII contributors had not established specific controls and procedures to enter complete data and discover erroneous data.

The DSS and the DCII contributors had not agreed upon and requested system features to require a unique identifier for records entered in the DCII. A unique identifier, such as a person's SSN, while not eliminating errors, could reduce errors and duplications in the database.

The DSS and DCII contributors did not have procedures or system features that required data in all fields, specifically the SSN field, to establish a DCII record. In addition, the system features did not include a listing of records or transactions with missing SSNs and a procedure to correct that situation.

The ASD (C^3I) had not directed DSS or DCII contributors to comply with OPM guidelines and DoD payroll practice procedures for constructing pseudo SSNs. In addition, system features did not include a means of flagging invalid SSNs that were created by using repeating or consecutive numbers (for example, all 2s or 123-45-6789).

Effects of the DCII on User Productivity and Confidence

As a result of procedural and functional limitations, many DCII contributors considered the DCII data unreliable. Rather than use data that they did not trust from the DCII to populate the Joint Personnel Adjudication System, DSS and the CAFs forwarded daily transactions directly to the Joint Personnel Adjudication System PMO.

Productivity of Adjudicators. According to CAF adjudicators, they had difficulty ordering case files and using the DCII error report after DSS transferred data processing to the Corporate Enterprise System. CAF personnel did not use the DCII error report because it was voluminous and did not include corrections. For batch transmissions, the DCII error report printed a cumulative alpha listing without the date of transactions. To ensure that daily batch transactions were recorded in the DCII, adjudicators kept a manual record of their adjudicative determinations. The adjudicators would check the DCII after a couple of days to ensure that their adjudicative determinations were recorded. When errors were found, the adjudicators had to request CAF senior management to correct the record.

The CAF adjudicators also reported that multiple records for an individual caused data entry problems during batch processing. Specifically, the DCII could not determine which record to update or delete among multiple records for an individual. The DCII would print out a message in the error report such as "Unexpected Add Failure." CAF personnel would have to manually update those records. DSS personnel submitted system change requests to the DSS Information Technology PMO to correct batch processed updates as the CAFs requested. However, the PMO had not reported estimated product delivery dates to DSS for those changes.

Security officers at DoD organizations use the DCII to verify security clearance eligibility and access granted to a job applicant, contractor, or employee. The DCII allows security officers to check the status of personnel security investigations to determine whether an investigation was opened or completed,

the type of investigation, and whether it was favorable. If any DCII information is inaccurate, security officers could inadvertently approve hiring individuals or granting access to individuals who should not have access. The Washington Headquarters Service CAF personnel reported frequently receiving calls from field security officers who used the DCII web-based option to verify individuals' security clearance eligibility. The security officers called the CAF because they were unable to find current information on individuals in the DCII. Using the DCII client-server option, the CAF personnel were able to provide needed information on the individuals to the security officers. The inability to quickly access information from the DCII could impede the security officer's decision to grant access to a person.

Identification of Individuals Requiring Periodic Reinvestigations. General Accounting Office Report No. NSIAD-00-215, "DoD Personnel: More Actions Needed to Address Backlog of Security Clearance Reinvestigations," August 24, 2000, states that the DCII does not have the capability to identify individuals in need of periodic reinvestigations because the information in the DCII is unreliable. The DCII can provide a rough estimate of the backlog; however, the DCII overstates the backlog because it includes many individuals who are:

- no longer employed by DoD,
- eligible for clearance but no longer require access to classified information, and
- accessing information at a lower classification level than the highest eligible classification level shown for them.

The General Accounting Office report states that the DCII had too much unreliable information, which cluttered up the database and created problems for the Defense agencies when they tried to get an accurate count of individuals needing a periodic reinvestigation.

Conclusion

DoD and non-DoD organizations use the DCII to verify investigative and security clearance eligibility information on DoD military, civilian, and contractor personnel. DCII users need accurate and reliable information in the database to facilitate sound decisions regarding the eligibility of DoD and contractor personnel to have access to classified and sensitive information. DoD criminal and security investigative personnel use the DCII to index their investigative data. The DoD CAFs and criminal investigation agencies rely on DCII information to perform their missions. DSS needs to implement controls and procedures that reestablish DCII data integrity to a level of reasonable accuracy and reliability if using organizations are to make informed security related decisions on personnel.

Management Comments on the Report and Audit Response

Although not required to comment, the Naval Criminal Investigative Service provided comments on the draft report. A summary of management comments on the report and our response are in Appendix D. For the full text of the the Naval Criminal Investigative Service comments, see the Management Comments section of the report.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence):

a. Establish a person's social security number as a unique personal identifier to record investigative results and security clearance eligibility and access determinations in the Defense Clearance and Investigations Index.

b. Reestablish the request for a quarterly analysis of the Defense Clearance and Investigations Index by the Defense Manpower Data Center to identify potential candidates for purging.

A.2. We recommend that the Director, Defense Security Service:

a. Modify the Defense Clearance and Investigations Index to:

(1) Mass delete obsolete investigative dossiers and clearance tracings.

(2) Accept batch transmissions of personnel security investigation cases from all contributors who need batch transmissions.

(3) Check the social security number field for valid content to the extent possible.

b. Establish procedures to:

(1) Periodically compare codes and instructions in the Defense Clearance and Investigations Index Users' Manual to Federal and DoD codes and actual operations to update the manual and operations to accommodate changes appropriately.

(2) Incorporate Federal guidance in the Federal Information Processing Standards for country codes.

Management Comments. The Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and

Intelligence), and the Director, Defense Security Service, did not comment on a draft of this report. We request that the Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director, Defense Security Service, provide comments on the final report.

Naval Criminal Investigative Service Comments. Although not required to comment, the Naval Criminal Investigative Service disagreed with Recommendation A.1.a., stating that forcing criminal investigators to enter complete personal identification data would prevent investigative agencies from entering investigations in the DCII as required by regulations and instructions. The Naval Criminal Investigative Service further stated that social security numbers given to investigators may be incorrect or fraudulent. The Naval Criminal Investigative Service concurred with the need for Recommendations A.1.b. and A.2.

Audit Response. We disagree that use of social security numbers as unique identifiers would prevent entering investigations in DCII. It is customary for processing systems to produce error listings on incomplete entries and for users to have an established methodology for handling those errors. The same could be established for investigations without social security numbers. We believe that a person is no more likely to provide an incorrect or fraudulent social security number than to provide a variation on name or other personal identification information that would generate an unmatched record in the DCII.

B. Pseudo Social Security Numbers for Foreign Nationals

The Defense Security Service Operation Center–Columbus (DSSOC-C) assigned over 1,400 pseudo SSNs of which 524 were inconsistent and did not conform to Office of Personnel Management (OPM) guidance. In addition, DSSOC-C had a cumbersome process to track pseudo SSNs assigned to foreign nationals. The DSSOC-C did not properly assign or effectively track pseudo SSNs because DoD security regulations had no guidance to implement OPM guidance or to require tracking pseudo SSNs. As a result, foreign nationals were inadequately identified in the DCII and multiple foreign nationals were assigned the same pseudo SSN.

Reason for Assigning Pseudo SSNs

In addition to indexing U.S. citizens with personnel security and criminal investigations, the DCII indexes foreign nationals granted Limited Access Authority (LAAs). The DoD issues LAAs that grant access to classified information when it has compelling reasons to do so in furtherance of the DoD mission. Unlike U.S. citizens, foreign nationals employed by the Government do not have SSNs. The employing agency must devise a pseudo SSN for pay and personnel action purposes. OPM issued guidance on constructing pseudo SSNs for use in Government agencies' personnel databases.

Guidance on Assigning Pseudo SSNs

Office of Personnel Management Guidance. As early as 1983, the OPM Operating Manual gave permission to Federal agencies to create pseudo SSNs when valid SSNs were not available. The 1983 version of the OPM Manual advised agencies to construct a 9-digit pseudo SSN.

The 1994 revision of the OPM manual provided guidance on how to construct a pseudo SSN. The manual stated that the lead digit should be either an 8 or 9, which are numbers that the Social Security Administration would not use for valid SSNs. To construct the pseudo SSN, a Federal agency would follow the 8 or 9 with a 4-digit personnel office identification number assigned by OPM. The personnel office of the Federal agency would assign the last 4 digits in sequential order to complete the pseudo SSN. By following the OPM procedure for constructing pseudo SSNs, Federal personnel offices ensure that each employee requiring a pseudo SSN is assigned a unique number. The OPM procedure for assigning pseudo SSNs appears in Chapter 4, "Requesting and Documenting Personnel Actions," of the January 2, 2000, update 33 of the OPM Operating Manual.

DoD Financial Management Guidance. Although security guidance does not discuss assignment of pseudo SSNs, DoD Regulation 7000.14-R, "DoD Financial Management Regulation," volume 8, "Civilian Pay Policy and

Procedures," August 1999, does. The financial management regulation requires that employee pay records use the SSN to identify all employees paid by the DoD. When an employee does not have a valid SSN, payroll offices must use a pseudo SSN to identify the individual on employee pay records. The financial management regulation requires use of the OPM Operating Manual in administering civilian pay and leave.

Foreign Nationals Certified for LAAs by Military Departments

According to the Military Departments' annual reports on LAAs granted, 12 of 302 foreign nationals with LAAs also had an assigned pseudo SSN. The number of foreign nationals certified for LAAs by each Military Department, according to the most recent report, was as follows:

- **Department of the Army.** At the end of FY 2000, the Army had validated 35 foreign nationals for LAAs. Of those 35, 12 were indexed in the DCII using a personal identification number.

- **Department of the Navy.** At the end of FY 2000, the Navy had validated 230 foreign nationals for LAAs. Of those 230, none were indexed in the DCII using a personal identification number. The Navy uses name, date of birth, and place of birth to identify foreign nationals.

- **Department of the Air Force.** As of FY 1999, the Air Force had validated 37 foreign nationals for LAAs. Of those 37, none were indexed in the DCII using a personal identification number.

Foreign Nationals Indexed in the DCII

In January 2000, DMDC analyzed 8,717 DCII records that had invalid or blank SSNs to identify those records for foreign nationals. The analysis identified 503 invalid SSNs and 1,837 blank SSN records as records of foreign nationals. DMDC matched only one foreign national indexed in the DCII with a record in the DoD personnel databases.

DSSOC-C Procedures for Assigning Pseudo Social Security Numbers for Limited Access Authority

The Director, Security Programs, ASD(C^3I), had not directed implementation of OPM guidance for constructing pseudo SSNs for foreign nationals granted LAA

to DoD classified information. In addition, the Director had not provided guidance on indexing and tracking foreign nationals assigned pseudo SSNs in the DCII.

DSSOC-C (formerly Defense Industry Security Clearance Office) began assigning pseudo SSNs in 1980 to process and index personnel security investigations of and security eligibility and access granted to foreign nationals. Personnel assigned to the International Branch, DSSOC-C, stated that DSS had no formal procedures for assigning pseudo SSNs. According to DSSOC-C documentation, DSSOC-C began assigning pseudo SSNs with the number 000-00-8650. As of July 19, 2000, DSSOC-C had assigned 1,433 pseudo SSNs to foreign nationals and the last number assigned was 000-11-0029.

The DSSOC-C personnel responsible for assigning and tracking pseudo SSNs for foreign nationals developed an organizational procedure for assigning the SSNs. When a request came in for a pseudo SSN, the first step was to determine the last pseudo SSN assigned and then check the DCII to determine whether the next sequential number was unassigned. If the next sequential number was unassigned, the foreign national needing a pseudo SSN was assigned that number.

DSSOC-C maintained records on foreign nationals assigned pseudo SSNs on manually prepared lists. The information recorded on the lists, in many instances, was not legible. Also, the personal information recorded for the foreign nationals, in many instances, was not sufficient to provide adequate identification of the individual. For 524 of the 1,433 foreign nationals listed, DSSOC-C did not have the foreign nationals' date of or place of birth recorded. The records showed that 151 foreign nationals were assigned to a total of 69 pseudo SSNs; therefore, more than one foreign national was assigned the same pseudo SSN.

Responsibility for Assigning Pseudo SSNs to Foreign Nationals

DoD 5200.2-R requires that overseas DoD commands prepare and submit DD Form 1879 or an Electronic Personnel Security Questionnaire to request and initiate a personnel security background investigation for foreign nationals requiring LAA. We believe that the overseas commands' security offices or personnel offices should construct a pseudo SSN in accordance with OPM guidance and enter it on the request-for-investigation form if the foreign national was not previously assigned a pseudo SSN. Assigning and tracking the pseudo SSN at the overseas command level should ensure that each foreign national would be assigned a unique personal identification number.

For foreign nationals working in the United States at DoD or contractor facilities without an SSN and requiring LAA, DSSOC-C should assign a pseudo SSN until the foreign national receives a valid SSN from the Social Security Administration. That pseudo SSN assigned by DSSOC-C should also conform to OPM guidance. When a foreign national receives a valid SSN, the security officer at the DoD or contractor organization should submit the number to DSSOC-C so that the foreign national's record in the DCII can be updated.

Correcting Pseudo SSNs Assigned to Foreign Nationals

DoD Regulation 7000.14-R, "DoD Financial Management Regulation," volume 8, "Civilian Pay Policy and Procedures," August 1999, requires that employee pay records use the SSN to identify all employees paid by the DoD. When an employee is not required to have an SSN, payroll offices must use a pseudo SSN to identify the individual on employee pay records. We believe that accurately identifying foreign nationals granted LAA in the DCII is as important as accurately identifying them for payroll purposes. Any foreign national employed by DoD should already have a pseudo SSN for payroll purposes that conforms to OPM guidance and that same number should be used for security purposes. To reconstruct DCII records of foreign nationals reported to the Director, Security Programs, ASD(C^3I), for FY 2000, the CAFs should obtain the pseudo SSN assigned to the individuals by the overseas major commands' payroll officers and enter those numbers in the DCII. If a DoD contractor assigned to an overseas major command employs the foreign national, the appropriate Military Department CAF should request DSSOC-C to construct and assign the contractor-employed foreign national with a pseudo SSN that conforms to OPM guidance. The CAF should correct the foreign national's SSN data field with the new pseudo SSN.

Conclusion

DoD established procedures to initiate personnel security investigations for foreign nationals requiring LAA. However, the DoD procedures did not implement OPM guidance for constructing a pseudo SSN for foreign nationals requiring LAA. Foreign nationals working at overseas major commands are required to have an appropriately constructed pseudo SSN for DoD payroll purposes. To improve processes and information, we believe the same number should be used for personnel security purposes.

Recommendations, Management Comments, and Audit Response

B. We recommend that the Director, Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence):

1. Revise DoD Regulation 5200.2-R, "Department of Defense Personnel Security Program," to implement the Office of Personnel Management's guidance on constructing pseudo social security numbers for foreign nationals requiring limited access authority.

2. Require DoD central adjudication facilities or other organizations establishing records in the Defense Clearance Investigations Index to

determine the pseudo social security numbers assigned to foreign nationals for DoD payroll purposes, and use those numbers in the Defense Clearance and Investigations Index.

Management Comments. The Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director, Defense Security Service, did not comment on a draft of this report. We request that the Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director, Defense Security Service, provide comments on the final report.

Naval Criminal Investigative Service Comments. Although not required to comment, the Naval Criminal Investigative Service disagreed with Recommendation B.2., stating that the Chief of Naval Operations is the focal point for limited access authorizations within the Department of the Navy.

Audit Response. We added wording to the recommendation to allow for organizations other than the central adjudication facilities to determine pseudo social security numbers for circumstances in which the central adjudication facility does not establish the foreign national's record in the DCII.

Appendix A. Audit Process

Scope and Methodology

We reviewed and evaluated the accuracy, availability, integrity and timeliness of information in the DCII. We interviewed personnel from DSS-Linthicum, Joint Personnel Adjudication System PMO, DoD central adjudication facilities, and criminal investigative agencies to determine their concerns with the database. We also met with personnel from the office of the Director, Security Programs, ASD(C^3I) and the DSS PMO. We reviewed applicable DoD and DSS regulations and guidelines to determine the responsibilities of the Director, Security Programs, ASD(C^3I); DSS; and DCII contributors for establishing and implementing policy for the operation and maintenance of the DCII database and for entering and updating information in the database. Specifically, we collected and reviewed operating procedures for the DCII; correspondence with personnel at the DSS, DCII CAFs, and contributors; and various DCII records.

To assess the accuracy and integrity of the DCII information, we reviewed personal identification data fields for 8,717 individuals who were indexed in the DCII with clearance tracings, but who had blank or invalid SSNs. The DCII had 24 million individuals indexed in its database, of which 2.4 million were indexed with clearance tracings. We reviewed documentation dated from November 1980 through December 2000. We also evaluated the process that DSS used to assign pseudo SSNs to foreign nationals by discussing the process with DSSOC-C personnel and reviewing DSSOC-C documents that listed 1,433 foreign nationals with assigned pseudo SSNs.

We did not evaluate the Management Control Program as a whole. We limited our review to DSS application and physical and system access security controls for the DCII. Specifically, we reviewed actions taken by the Director, Security Programs, ASD(C^3I); DSS; DSS Information Technology PMO; and DCII contributors to provide reasonable assurance of the accuracy and reliability of inputs, processing, and outputs in the DCII. We also reviewed management's observance of applicable laws, regulations, and policies.

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following objectives and goal, subordinate performance goal, and performance measure.

> **FY 2001 DoD Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure **(01-DoD-02)**.

FY 2001 Subordinate Performance Goal 2.5: Improve DoD financial and information management **(01-DoD-2.5)**. **FY 2001 Performance Measure:** Qualitative Assessment of Reforming Information Technology (IT) Management **(01-DoD-2.5.3)**.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Use of Computer-Processed Data. To achieve the audit objectives, we relied on computer-processed data provided by the DMDC, which was generated from DCII and DoD military and civilian personnel databases. We did not perform tests of system general and application controls to confirm the reliability of the data. However, when we reviewed the data in context with other available evidence, we believe that the opinions, conclusions, and recommendations in this report are valid.

Audit Type, Dates, and Standards. We conducted this economy and efficiency audit from March 2000 through January 2001, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We comply with Government Auditing Standards except for the requirement for an external quality control review. Measures have been taken to obtain an external quality control review.

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

Appendix B. Prior Coverage

During the past 5 years, the General Accounting Office issued two reports and the Office of the Inspector General, DoD, issued seven reports discussing the DCII and other security related issues. General Accounting Office unrestricted reports can be accessed over the Internet at http://www/gao.gov. Office of the Inspector General, DoD, unrestricted reports can be accessed over the Internet at http://www.dodig.osd.mil/audits/reports. Specific reports related to this audit are listed below.

General Accounting Office

General Accounting Office Report No. NSIAD-00-215 (OSD Case No. 2055), "DoD Personnel; More Actions Needed to Address Backlog of Security Clearance Reinvestigations," August 24, 2000

General Accounting Office Report No. NSIAD-00-12 (OSD Case No. 1901), "DoD Personnel; Inadequate Personnel Security Investigations Pose National Security Risks," October 27, 1999

Inspector General, DoD

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

Inspector General, DoD Report No. D-2001-019, "Program Management of the Defense Security Service Case Control Management System," December 15, 2000

Inspector General, DoD, Report No. D-2001-008, "Resources of DoD Adjudication Facilities," October 30, 2000

Inspector General, DoD, Report No. D-2000-134, "Tracking Security Clearance Requests," May 30, 2000

Inspector General, DoD Report No. D-2000-111, "Security Clearance Investigative Priorities," April 5, 2000

Inspector General, DoD, Report No. D-2000-072, "Expediting Security Clearance Background Investigations for Three Special Access Programs" (U), January 31, 2000 (SECRET)

Inspector General, DoD Report No. 98-124, "Department of Defense Adjudication Program," April 27, 1998

Inspector General, DoD Report No. 98-067, "Access Reciprocity within DoD Special Access Programs," February 10, 1998 (SECRET)

Appendix C. Defense Clearance and Investigations Index Contributors and Non-Department of Defense Users

DCII Major Contributors

Air Force Central Clearance Facility

Air Force Office of Special Investigations

Army Central Clearance Facility

Army Crime Records Center

Army Investigative Records Repository

Defense Intelligence Agency

Defense Office of Hearing and Appeals

Defense Security Service

Inspector General, Department of Defense

Joint Chiefs of Staff

Naval Central Clearance Facility

Naval Criminal Investigative Service

National Reconnaissance Office

National Security Agency

Washington Headquarters Service

Non-DoD Users

Central Intelligence Agency

Department of Energy (Headquarters)

Department of State

Non-DoD Users (cont.)

Department of Treasury

Federal Bureau of Investigation

National Aerospace and Space Administration

Office of Personnel Management

United States Coast Guard

Appendix D. Audit Response to Naval Criminal Investigative Service Comments Concerning the Report

Our detailed responses to the comments of the Assistant Director for Inspections, Naval Criminal Investigative Service, on the draft report follow. The complete text of those comments is in the Management Comments section of this report.

Naval Criminal Investigative Service Comments. The Naval Criminal Investigative Service was dissatisfied with the audit report coverage on three issues. The issues that the Naval Criminal Investigative Service considered concerns that the report should have addressed were DCII responsiveness, DCII reports, and resolution of DCII system problems.

Audit Response. The report does discuss DCII responsiveness, DCII reports, and resolution of DCII system problems. The examples provided may not be specific to the Naval Criminal Investigative Service, but they do illustrate the concerns among the DCII contributor and user community.

DCII responsiveness and its effect on user productivity are discussed on page 9 under the subheading, "Effects of the DCII on User Productivity and Confidence."

DCII reports prepared to identify records that are candidates for deletion, which could be records that the comments describe as "aged out," are also discussed on page 7. The discussion was limited to the DCII reports identifying obsolete records. No reports other than the obsolete record report were brought to our attention as having a systemic, community-wide impact.

Resolution of system problems is discussed on page 6 under the subheading, "User Needs for DCII Capabilities." This section describes how other systems received higher priority than the DCII and how requests for changes and modifications went unanswered. Because we did not evaluate the priority system used for responding to information system problem reports, we did not recommend that the DCII receive a different priority.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director (Program Analysis and Evaluation)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director, Security
    Deputy Director, Personnel Security
General Counsel of the Department of Defense
  Deputy General Counsel, Legal Counsel
  Director, Defense Office of Hearing and Appeals
Director, Washington Headquarters Service
  Director, Directorate for Personnel and Security
    Chief, Consolidated Adjudication Facility

Joint Staff

Chairman, Joint Chiefs of Staff
Director, Joint Staff
Director of Management
  Chief, Joint Staff Security Office
    Chief, Personnel Security Branch

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief, Army Technology Management Office
Commanding General, Army Criminal Investigation Command
  Chief, Crimes Records Division
Commander, Army Investigative Records Repository
Commander, Total Army Personnel Command
  Adjutant General, The Adjutant General Directorate
    Commander, Army Central Personnel Security Clearance Facility
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Chief of Naval Operations
  Director, Special Programs Division
Naval Inspector General

Department of the Navy (cont'd)

Auditor General, Department of the Navy
Director, Naval Criminal Investigative Service
    Director, Central Adjudication Facility

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Administrative Assistant to the Secretary of the Air Force
    Director, Security and Special Programs Oversight
    Director, Air Force Central Adjudication Facility
Auditor General, Department of the Air Force
Commander, Air Force Office of Special Investigations

Other Defense Organizations

Director, Defense Intelligence Agency
    Director, Directorate for Administration
        Chief, Counter Intelligence and Security Activities
            Chief, Central Adjudication Facility
    Inspector General, Defense Intelligence Agency
Director, Defense Security Service
    Inspector General, Defense Security Service
    Director, Defense Industrial Security Clearance Office
Director, National Reconnaissance Office
    Director, Security Service
        Chief, Central Adjudication Facility
    Inspector General, National Reconnaissance Office
Director, National Security Agency
    Director, Security Services
        Chief, Personnel Security Analysis
            Chief, Central Adjudication Facility
    Inspector General, National Security Agency

Non-Defense Federal Organizations

Office of Management and Budget

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 Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Mangement, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform
House Permanent Select Committee on Intelligence

Naval Criminal Investigative Service Comments

DEPARTMENT OF THE NAVY

HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
WASHINGTON NAVY YARD BLDG 111
716 SICARD STREET SE
WASHINGTON DC 20388-5380

5230
Ser 006/1U0006
12 April 2001

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE (ATTN: Acquisition Management Directorate)

Subj: DEFENSE CLEARANCE AND INVESTIGATIONS INDEX DATABASE (PROJECT NO. D200AD-0132)

Ref: (a) DODIG Draft of Proposed Audit Report dtd 15 Feb 2001

1. In response to reference (a), the following input is formatted to address the recommendations therein. Further, additional comments are included which are keyed toward findings reported via reference (a).

Recommendations

A.1. We recommend that the Director for Security Programs, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence):

a. Establish a person's social security number (SSN) as a unique personal identifier to record investigative results and security clearance eligibility and access determinations in the Defense Clearance Investigations Index.

NON-CONCUR: Ideally a person's SSN could be used as a unique personal identifier in DCII. While Central Adjudication Facilities (CAFs) should be able to validate SSN and other PID data for DCII entry, criminal investigators use the SSN given by the individual at the time of interview, which may be incorrect or fraudulent. The SSN utilized in the criminal investigation is entered into DCII. From a records management perspective, we have found it better to index the number contained in the report, even if suspect. To limit DCII entries to only those wherein complete PID data can be collected would prevent investigative agencies from making DCII entries as required by DOD Instruction 5505.7 and DOD 5200.2-R. Once DOD's Joint Personnel Adjudication System (JPAS) is fielded in late 2001, DCII will cease being the system of record for security clearance eligibility and access determinations.

b. Reestablish the request for a quarterly analysis of Defense Clearance and investigations Index by the Defense Manpower Data Center to identify potential candidates for purging.

CONCUR: Recommendation should further state this pertains to CAF clearance tracings to avoid confusion with need for annual roster of aged-out tracings of investigative files maintained by records centers. As a practical matter this would serve to maintain only viable information in the database.

A.2. We recommend that the Director, Defense Security Service:

a. Modify the Defense Clearance and Investigations Index to:

(1) Mass delete obsolete investigative dossiers and clearance tracings.

CONCUR: Maintain only viable and accurate records in the database.

(2) Accept batch transmissions of personnel security investigation cases from all contributors who need batch transmissions.

CONCUR: Batch processing allows for a quick and complete transmission of information so that the users in the security community may be assured that the data relied upon when making security determinations is accurate and up to date.

(3) Check the social security number field for valid content to the extent possible.

CONCUR: Validating content in the SSN field will provide assurances that the information is accurate.

b. Establish procedures to:

(1) Periodically compare codes and instructions in the DCII Users Manual to Federal and DOD codes and actual operations to update the manual and operations to accommodate changes appropriately.

CONCUR: To ensure accuracy and maintain reciprocity between DOD and other Federal agencies.

Final Report Reference

(2) Incorporate Federal guidance in the Federal Information Processing Standards for country codes.

CONCUR: To standardize and resolve any conflicting or absent codes.

B.1. Revise DOD Regulation 5200.2-R, "Department of Defense Personnel Security Program," to implement the Office of Personnel Management's guidance on constructing pseudo social security numbers for foreign nations requiring limited access authority.

NO COMMENT: Responsibility for revision of DOD regulation does not fall within NCIS.

B.2. Require DOD central adjudication facilities to determine the pseudo social security numbers assigned to foreign nationals for DOD payroll purposes and use those numbers in the Defense Clearance and Investigations Index.

NONCONCUR: The Chief of Naval Operations (OP09N) is the focal point for limited access authorizations within the Department of the Navy and not the CAF. Revised

2. Page 7, "Mass Deletion of Obsolete Dossiers and Clearance Tracings": delete the phrase "and clearance" from the second paragraph, third sentence. NCIS Records Management Division (RMD) manages investigative dossiers and tracings; DONCAF manages DCII clearance tracings. The 18,759 files deleted were investigative dossiers and tracings deleted by RMD. Revised

3. Page 8, "Requested Adjudicative Dossier Line". The addition of tracings to dossiers is the function of the supporting records center. Within Department of the Navy, DONCAF forwards supplemental adjudicative material to RMD where the material is filed within the adjudicative dossier and DCII tracing updated by RMD.

4. On several occasions DODIG personnel interviewed individuals from the NCIS Records Management Division (RMD). The major thrust of their comments was two-fold, yet neither of their issues was addressed in the draft audit report. Discussions among leaders of other DOD record centers reveal that the concerns expressed by NCIS are common to the other records centers. The omission of these issues is seen as a major shortcoming of the audit and contributes to the continued deficiencies of the DCII, particularly its accuracy and

timeliness. Without addressing these concerns in the report, it is difficult to see how any effort to fix the DCII's many problems can be successful.

a. DCII Responsiveness: With the deployment of the Corporate Enterprise System (CES) in 1998, the time it took to add, delete or modify a DCII tracing increased significantly. Pre CES transactions could be completed in seconds. Now it takes much longer; frequently up to several minutes. Additionally, the process requires more steps and is cumbersome. Maintenance of DCII entries is a major contributor responsibility. As commented on throughout the audit report, the accuracy of the DCII is of paramount importance if the database is to be trusted by its users. With the degradation of service after CES, agencies' ability to add, modify and delete DCII tracings was seriously eroded. Personnel staffing decisions are traditionally based on historical data tied to the number of transactions to be worked and the average time it took to complete a typical transaction. CES made obsolete all such staffing decisions. Now it takes much longer, up to double or triple the time, to complete a single transaction. Yet, due to personnel ceilings, authorizations for additional personnel to address DCII update issues have not been favorably received. This is a major cause of the huge number of obsolete or inaccurate tracings remaining in the DCII, sometimes for years. Since additional personnel to complete DCII transactions appears out of the question, the solution is for the DCII to process transactions faster and more simply. The recommendation for bulk deletion, while helpful for some, is not going to resolve this issue. Some agencies, such as NCIS for its investigative tracings, cannot use bulk deletions.

b. DCII Reports: Prior to the deployment of CES, the DCII provided the records centers a number of reports. These reports addressed a number of issues and were either periodic or aperiodic (i.e., provided upon specific request). Some were common to all the records centers. One such report was the annual report of files that, according to the year index and the retention code as contained in the file tracing, had aged out. This report was to be furnished to each records center contributor annually in the month of January. The report was used to locate records so that they could be reviewed. If they had in fact aged-out in accordance with the agency's records disposition manual (as approved by the Archivist of the United States), then the file was deleted (or, if permanent, transferred to the National Archives) and the DCII tracing(s) deleted. Other reports were created specifically for use by one or several of the records centers. Such a report might be a breakout of the record center's holdings. This enable records

centers to determine the composition of their holdings by record type (e.g., adjudicative, investigative, etc.), year index, disposition code, etc. These reports helped the record officer more efficiently manage the records. Sometimes, the DCII provided special reports needed for a limited purpose, but to support operations or improvement of records and DCII entry management. With the deployment of CES, DSS' ability to provide these reports ceased. The May 1999 meeting of the DCII Users Counsel addressed this issue. A working group was established with the NCIS Records Officer as the leader. The group has met once and is developing a list of periodic and special reports that it wants DCII to develop and provide. DSS action to develop programs to provide these reports will enable contributing records centers to more efficiently manage their DCII tracings. Support for this effort should be contained in Part A, page 11, Recommendations, paragraph A.2a.

c. DCII System Problems Resolution: Shortly after the deployment of the CES system, NCIS began to encounter problems with the DCII. We generally notified the DCII Help Desk and also discussed this with other DCII personnel. While some issues were resolved, others persist. One such example involves problems deleting some tracings from the DCII. The DCII rejected the attempt to delete and displayed the following response: "DISCORP.TRACING_ FILE_DEMAND_MANAGER_FK) VIOLATED-CHILE RECORD FOUND." Local analysis determined that this situation occurs when there is also a DCII on-line demand for the file. This problem was forwarded to DCII nearly two years ago. It was also raised at the May 1999 DUC meeting, but remains unresolved. Currently, there are several hundred tracings that have aged-out that cannot be deleted. Our inability to delete these tracings means they remain in the DCII even though in some cases the associated files have been destroyed. It is issues like this and other similar issues that DSS has been unable to resolve that also contribute to an inaccurate DCII database.

5. Points of Contact on this issue are: Ms. Fredericka Oar, Code 29D, Telephone: (202) 433-8885, as it relates to the CAF; and Mr. Henry Persons, Code 27D, Telephone: (202) 433-9505, as it relates to records management.

Veronica McCarthy

VERONICA MCCARTHY
Assistant Director
For Inspections

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector, DoD, who contributed to the report are listed below.

Mary L. Ugone
Robert K. West
Judith I. Padgett
Walter L. Jackson
Bryon J. Farber
Heather L. Jordan
Jacqueline Pugh