

Naval Audit Service



Audit Report



Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Selected Activities

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

*Do not release outside the Department of the Navy
or post on non-NAVAUDSVC Web sites
without prior approval of the Auditor General of the Navy*

N2011-0024

11 March 2011

Obtaining Additional Copies

To obtain additional copies of this report, please use the following contact information:

Phone: (202) 433-5757
Fax: (202) 433-5921
E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits, please use the following contact information:

Phone: (202) 433-5840 (DSN 288)
Fax: (202) 433-5921
E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

<http://secnavportal.donhq.navy.mil/navalauditservices>

Guide to Acronyms

DON	Department of the Navy
DON CAF	Department of the Navy Central Adjudication Facility
JPAS	Joint Personnel Adjudication System
NCIS	Naval Criminal Investigative Service
SECNAV	Secretary of the Navy
SF	Standard Form



DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
N2009-NFO000-0056
11 Mar 11

MEMORANDUM FOR DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE

Subj: EFFECTIVENESS OF THE DEPARTMENT OF THE NAVY’S DENIAL PROCESS FOR INTERIM SECURITY CLEARANCES AT SELECTED ACTIVITIES (AUDIT REPORT N2011-0024)

Ref: (a) Naval Audit Service memo N2009-NFO000-0056, dated 29 October 2009
(b) Secretary of the Navy Instruction 7510.7F, “Department of the Navy Internal Audit”

1. The report provides results of the subject audit announced in reference (a). Section A of this report provides our findings and recommendations, summarized management responses, and our comments on the responses. Section B provides the status of the recommendations. The full text of management responses is included in the Appendix. The Office of the Director, Naval Criminal Investigative Service was the action command for all recommendations.

2. Actions planned by the Naval Criminal Investigative Service meet the intent of the recommendations. The recommendations are considered open pending completion of the planned corrective actions, and are subject to monitoring in accordance with reference (b). Management should provide a written status report on the recommendations within 30 days after target completion dates, and also within 30 days of the interim target dates provided for Recommendations 1-4 and 6-8. Please provide all correspondence to the Assistant Auditor General for Manpower and Reserve Affairs Audits, XX, with a copy to the Director, Policy and Oversight, XX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)

3. Any requests for this report under the Freedom of Information Act must be approved by the Auditor General of the Navy as required by reference (b). This audit report is also subject to followup in accordance with reference (b).

Subj: **EFFECTIVENESS OF THE DEPARTMENT OF THE NAVY'S DENIAL
PROCESS FOR INTERIM SECURITY CLEARANCES AT SELECTED
ACTIVITIES (AUDIT REPORT N2011-0024)**

4. We appreciate the cooperation and courtesies extended to our auditors.



XXXXXXXXXXXXXXXXXXXX
Assistant Auditor General
Manpower and Reserve Affairs Audits

FOIA (b)(6)

Copy to:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N40, N41)
CMC (RFR, ACMC)
DON CIO
NAVINGEN (NAVIG-4)
AFAA/DO

Table of Contents

EXECUTIVE SUMMARY	1
Overview	1
Reason for Audit.....	2
Noteworthy Accomplishments	2
Communication With Management	3
Federal Managers’ Financial Integrity Act	3
Corrective Actions.....	3
 SECTION A: FINDINGS, RECOMMENDATIONS, AND CORRECTIVE ACTIONS	 5
Finding 1: Granting Interim Clearances.....	5
Audit Results	5
Recommendations	7
 Finding 2: Debriefing Upon DON CAF Denial.....	 10
Audit Results	10
Recommendations	11
 SECTION B: STATUS OF RECOMMENDATIONS	 14
 EXHIBIT A: SCOPE AND METHODOLOGY	 17
 EXHIBIT B: ACTIVITIES VISITED AND/OR CONTACTED.....	 19
 APPENDIX: MANAGEMENT RESPONSE FROM DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE.....	 20

Executive Summary

Overview

We concluded that the Department of the Navy (DON) did not effectively process civilian and military interim clearances, properly and efficiently manage subsequent DON Central Adjudication Facility (DON CAF) denials, or sufficiently mitigate the risk of access to classified information after denials. Our analysis of 340 DON-wide interim denial records¹ in the Joint Personnel Adjudication System (JPAS) as of 21 January 2010 showed that, contrary to Secretary of the Navy (SECNAV) guidance, DON commands granted interim clearances to individuals who disclosed adverse information on their Standard Form (SF) 86, “Questionnaire for National Security Positions.” Further, DON security managers did not debrief these individuals immediately upon DON CAF denial in accordance with SECNAV Manual M-5510.30, “DON Personnel Security Program,” dated June 2006.² Without debriefing these individuals, there is a risk that they will have continued access to classified information and not be informed of their legal responsibility to permanently safeguard the classified information they may have already accessed. Management practices that allowed these conditions to occur included: no interim clearance oversight policies and procedures, weak internal controls over the granting of interim clearances, contrary instructions, and insufficient security manager training.

Once implemented, the recommendations contained in this report should improve internal controls over the granting of interim clearances, provide for the implementation of sufficient oversight to ensure individuals are debriefed immediately upon notification of DON CAF denial, and ensure DON security managers receive proper training and refresher training.

The objective of DON’s Personnel Security Program is to authorize initial and continued access to classified information and/or assignment to sensitive duties to those persons whose loyalty, reliability, and trustworthiness are such that entrusting them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security.

SECNAV is the DON agency head responsible under Executive Orders 12968 and 10450 for establishing and maintaining an effective Personnel Security Program for all DON personnel. SECNAV has designated the Chief of Naval Operations, Special Assistant for

¹ See Exhibit A for information on our universe/sampling.

² We also referred to the SECNAV M-5510.30 as the “Manual” or “Security Manual” within this report.

Naval Investigative Matters and Security (N09N), who functions primarily as the Director, Naval Criminal Investigative Service (NCIS), as the senior security official for DON.³

Every command⁴ in DON eligible to receive classified information is required to designate a security manager responsible for managing the program and initiating the appropriate investigations of DON personnel. The Office of Personnel Management performs the investigations which include extended coverage of the subject's background in order to obtain a complete picture of the individual's character, loyalty, trustworthiness, and reliability.

DON CAF, an NCIS organization, determines eligibility for access to classified information based on the results of the Office of Personnel Management investigation and application of the adjudicative guidelines contained in SECNAV M-5510.30. There are many conditions that could raise an area of concern regarding an individual's loyalty, reliability, and trustworthiness to safeguard classified information, including foreign influence/preference, financial, personal conduct, and criminal issues.

We performed the audit from 10 November 2009 through 25 January 2011. Conditions noted existed during Fiscal Years 2009 and 2010.

During Fiscal Years 2009 and 2010, DON spent at least \$154 million and \$152 million, respectively, on its Personnel Security Program.

Reason for Audit

The audit objective was to verify that DON effectively and efficiently processed personnel security investigation requests for military and civilian personnel. Our specific audit focus was on interim clearances, subsequent DON CAF denials, and the risk of access to classified information.

This audit was initiated by the Naval Audit Service based on the Fiscal Year 2009 Risk and Opportunity Assessment submission addressing personnel security clearances.

Noteworthy Accomplishments

Prior to the audit, JPAS contained retired, deceased, or otherwise separated DON personnel. However, during the audit, the Head, Personnel Security Policy, Assistant for Information and Personnel Security, NCIS, coordinated with the Defense Security Service to implement a data quality initiative to reconcile JPAS to Bureau of Naval

³ "Director NCIS" is used throughout the report for ease of reading, and includes the dual function of N09N.

⁴ "Command" is any organizational entity including a unit, ship, laboratory, base, squadron, activity, facility, etc.

Personnel data. Specifically, Defense Security Service contracted through the General Services Administration to assist with a six-phase cleanup effort for the Navy JPAS data. NCIS worked as a liaison between the Bureau of Naval Personnel and the JPAS contractor to archive over 1.3 million Navy records. There is also a separate ongoing data quality initiative for the Marine Corps JPAS data.

Communication With Management

Throughout the audit, we kept the NCIS Inspector General, Head, Personnel Security Policy, and DON CAF senior officials informed of the conditions noted. Specifically, we communicated several times each month via e-mail and telephone calls. In addition, we conducted an entrance conference on 10 November 2009 with the NCIS Inspector General; Director DON CAF; NCIS Head, Personnel Security Policy, and the NCIS Comptroller.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1, 2, 6, 7, and 8 address issues related to the internal control over the granting of interim clearances and debriefing upon DON CAF denial. In our opinion, the weaknesses noted in this report may warrant reporting in the Auditor General's annual Federal Managers' Financial Integrity Act memorandum identifying management control weaknesses to the Secretary of the Navy.

Corrective Actions

To address the conditions noted in the report, we made recommendations to the Director, Naval Criminal Investigative Service to:

- Establish oversight policies and procedures for monitoring, inspecting, and reporting on the status/granting of interim accesses for DON, and revise Secretary of the Navy Manual-5510.30 accordingly.
- Revise Secretary of the Navy Manual-5510.30 to require commanding officers or designated security managers to review and certify, in writing, that no adverse information exists on the SF 86 prior to granting interim access to classified information, with memorandum being retained at the command for higher-level review or inspection as required.

- Develop mandatory security manager training addressing Secretary of the Navy Manual-5510.30 requirements and responsibilities, and ensure all new security managers promptly complete this training prior to granting an interim clearance.
- Revise Secretary of the Navy Manual-5510.30 to require security managers to take annual training, and provide documentation of course completion to a central oversight authority.
- Issue a “personal for” (P4) message to all commanding officers and security managers emphasizing that Secretary of the Navy Manual-5510.30 only permits the granting of interim access to classified information in the absence of adverse information disclosed on an SF 86. The P4 should also note the new certification, reporting, and training documentation requirements. In addition, the P4 message should address the Secretary of the Navy Manual-5510.30 requirements for the security managers to take the Naval Security Manager Course offered by the Naval Criminal Investigative Service.

Director, Naval Criminal Investigative Service concurred with the findings and recommendations and has planned corrective actions that meet the intent of the recommendations.

Section A:

Findings, Recommendations, and Corrective Actions

Finding 1: Granting Interim Clearances

Audit Results

Department of the Navy (DON) commands wrongly granted interim clearances to individuals who had disclosed adverse information⁵ on their Standard Form (SF) 86, “Questionnaire for National Security Positions.” This was contrary to Secretary of the Navy (SECNAV) Manual 5510.30, “Department of the Navy Personnel Security Program (PSP),” dated June 2006, which allows commanding officers⁶ to grant interim clearances to individuals pending completion of full investigative requirements and pending establishment of security clearance eligibility by the DON Central Adjudication Facility (DON CAF), in the absence of adverse information. Specifically, of 197 records with interim denials (i.e., clearances that were later denied by DON CAF) that were debriefed in a timely fashion,⁷ we estimate that at least 110⁸ had adverse information on their SF 86 that should have prevented the command from granting an interim clearance. Adverse information was also found on the SFs 86 for 19 of 22 (86 percent) judgmental samples taken from 143 records with interim denials that were not debriefed timely. Examples include:

- One of these individuals was granted an interim secret clearance by the local command and was subsequently denied eligibility by DON CAF. The individual had potential for access to classified information for at least 1,515 days even though he disclosed a DUI, an assault, wage garnishment, and being fired from a previous job on his SF 86. Further review of this individual’s Office of Personnel Management investigation file revealed over 24 previous arrests. According to his Commander, when the individual allegedly presented falsified Navy Reserve orders to get out of a civilian court date, the District Attorney contacted the Commander to verify the validity of the orders. As a result of our concurrent

⁵ Guidance regarding adverse information is contained in Appendix G of the Manual, and includes issues related to allegiance to the United States; foreign influence/preference; sexual behavior; personal conduct; financial considerations; alcohol consumption; drug involvement; emotional, mental, and personality disorders; and criminal conduct.

⁶ Commanding officers authorize, grant, limit, and control access to classified information, as appropriate; however, this responsibility is usually designated to the command security manager.

⁷ Finding 2 and Exhibit B provide further explanation on our universe and sampling.

⁸ This projection was calculated using a 90 percent confidence level based on a statistical sample of 20 interim denials debriefed in a timely fashion.

inquiries regarding this individual and a phone call from the District Attorney, the Commander began the process of administratively discharging the individual from the Navy Reserves. The Commander, who is also the security manager, was unable to answer our specific questions regarding the granting of the individual's interim clearance because the Commander had just arrived in May 2010.

- A second individual was granted interim top secret access by the European Central Command even though he disclosed a Ukrainian spouse and step-child in the Ukraine pending a custody agreement on his SF 86. His eligibility was subsequently denied by DON CAF; however, the individual had potential for access to classified information at the Sensitive Compartmented Information (SCI) level, including the Joint Worldwide Intelligence Communication System, for at least 540 days. The security manager for the European Central Command was new⁹ and could not answer our specific questions regarding the granting of this particular interim top secret clearance, although he indicated he was not responsible for granting it. Further, he was not able to determine actual access or specific top secret documents this individual may have had access to, since all read-ins¹⁰ are contained in an individual's Security Jacket, which had been destroyed 6 months after the individual left the command.¹¹
- A third individual was granted an interim secret access by the local command even though he disclosed a bankruptcy and other financial delinquencies, including his mortgage, student loan, and credit card, on his SF 86. His eligibility was subsequently denied by DON CAF; however, this individual had potential for access to classified information for 1,062 days. The security manager told us that although the individual had checked in with their command in February 2010, he had since transferred to another command. Since this security manager was not responsible for granting the interim clearance, the security manager could not provide responses to our specific questions regarding the granting of the interim clearance. The security manager was not able to provide the name of the security manager who granted the interim clearance.

Our judgmental sample of 22 records contained the following primary DON CAF reasons for denial: financial (14); alcohol (2); personal conduct (1); foreign influence (2); foreign preference (2); and criminal (1).

⁹ In his position for 2 months.

¹⁰ "Read-ins" is a term to describe the process used when a nondisclosure agreement is signed for each separate program accessed.

¹¹ We did not determine why the Security Jacket was destroyed after 6 months because that was outside our scope.

Management practices that allowed these conditions to occur include the following:

- There were no interim clearance oversight policies and procedures for the multiple DON commands that granted the accesses. Since DON CAF does not grant the interim clearances, they do not track or monitor them.¹²
- There were weak internal controls over the granting of interim clearances. For example, there was no requirement to certify that the SFs 86 did not contain any adverse information prior to granting the interim access.
- There was insufficient DON security manager training. For example, there were no requirements for annual refresher training, certification, or continuing professional education requirements for DON security managers. In addition, only 5 of 11 (45 percent) security managers responding to our questionnaire indicated they had completed the Naval Criminal Investigative Service's (NCIS's) formal required security manager training course.¹³

Allowing individuals who disclose adverse information on their SF 86 access to classified information is inconsistent with the interests of national security policy. It also creates an unnecessary risk to national security, which can result in significant human loss and financial cost. Further, there is a risk to DON's reputation in the event classified information is improperly disclosed by individuals who had inappropriately been granted interim clearances when adverse information previously existed.

Centralized monitoring of interim clearances should help provide uniformity among commands to ensure interim clearances are based on the absence of adverse information, security managers comply with training requirements, and debriefs are done on a timely basis.

Recommendations and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses are presented below. The complete text of the management responses is in the Appendix.

We recommend that the Office of the Director, Naval Criminal Investigative Service:

Recommendation 1. Establish oversight policies and procedures for monitoring, inspecting, and reporting on the status/granting of interim accesses for the Department of the Navy, and revise Secretary of the Navy Manual 5510.30 accordingly.

¹² DON CAF is responsible for performing the adjudication and determining eligibility for access to classified information. Local commands are responsible for granting access to classified information.

¹³ The NCIS training is a formal classroom training that is offered on a limited basis. Therefore, a new security manager may not have access to the training prior to being required to carry out their duties.

Management response to Recommendation 1. Concur. Open. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires the Secretary of the Navy Manual to be revised and issued. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 2. Revise Secretary of the Navy Manual 5510.30 to require commanding officers or designated security managers to review and certify, in writing, that no adverse information exists on the Standard Form 86 prior to granting interim access to classified information, with memorandum being retained at the command for higher-level review or inspection as required.

Management response to Recommendation 2. Concur. Open. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires the Secretary of the Navy Manual to be revised and issued. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 3. Develop mandatory security manager training addressing Secretary of the Navy Manual 5510.30 requirements and responsibilities, and ensure all new security managers promptly complete this training prior to granting an interim clearance.

Management response to Recommendation 3. Concur. Open. N09N2 will determine best method of ensuring the security managers accomplish required training. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires Secretary of the Navy Manual to be revised and issued. The policy change will include specific training requirements that need to be accomplished within 30 days of assumption of security manager duties. Preferred method is to use the Defense Security Service's existing online training resources to track and monitor completion of the requirements. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 4. Revise Secretary of the Navy Manual 5510.30 to require security managers to take annual training, and provide documentation of course completion to a central oversight authority.

Management response to Recommendation 4. Concur. Open. N09N2 will identify annual training requirements for security managers and determine best method of ensuring the training is accomplished and documented. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires Secretary of the Navy Manual to be revised

and issued. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 5. Issue a “personal for” (P4) message to all commanding officers and security managers emphasizing that Secretary of the Navy Manual 5510.30 only permits the granting of interim access to classified information in the absence of adverse information disclosed on an SF 86. The P4 should also note the new certification, reporting, and training documentation requirements. In addition, the P4 message should address the Secretary of the Navy Manual 5510.30 requirements for the security managers to take the Naval Security Manager Course offered by the Naval Criminal Investigative Service.

Management response to Recommendation 5. Concur. Open. N09N2 will draft and staff a suggested memorandum for the N09N. The P4 will remind commanders of the requirement to review the SF 86 information prior to issuing an interim security clearance. It will also remind commanders of the requirement for Security Managers to attend suitable training. The target completion date for the actions is 1 June 2011.

Naval Audit Service comment on responses to Recommendations 1-5. Actions planned by the Naval Criminal Investigative Service satisfy the intent of the recommendations, which are considered open pending completion of the actions.

Finding 2: Debriefing Upon DON CAF Denial

Audit Results

We found a significant number of instances when DON commands did not debrief those individuals granted interim clearances immediately upon DON CAF denial. Debriefs are important because they include ensuring all classified material in the individual's possession is returned, and require the individual to acknowledge that they are no longer eligible for access to classified information. SECNAV Manual 5510.30 states that once DON CAF makes an unfavorable eligibility determination (denial), the command must remove all accesses authorized and debrief the individual. Specifically we found:

- 143 of 340 (42 percent) interim clearances were not debriefed immediately upon DON CAF denial. Of the 143 who were not debriefed timely, 83 (58 percent) were never debriefed and 60 (42 percent) were debriefed late.
- The length of time from DON CAF denial date to debrief date (or date of data query for those who were never debriefed) was greater than 180 days for 70 of the 143 (49 percent) records.

Management practices that allowed these conditions to occur include the following:

Absence of Centralized Oversight of Interim Clearances. Since local commands granted the accesses, DON CAF did not track or monitor them. Therefore, when individuals needing to be debriefed had left a command, there was no central authority responsible for making sure they were properly debriefed.

Contrary Instructions. The DON CAF Letter of Intent¹⁴ and Letter of Notification¹⁵ contain instructions regarding debriefings¹⁶ that are not in accordance with SECNAV Manual 5510.30.

- The Letter of Intent states that “Per Chapter 8-4 of the Manual, any ‘interim’ or ‘temporary’ access must be immediately removed.” However, it does not address debriefs. Whereas, the Manual states that “...once the DON CAF [Central Adjudication Facility] makes an unfavorable eligibility determination,

¹⁴ The DON CAF Letter of Intent advises the individual of the proposed action, the reasons therefore, and the rebuttal process associated with the proposed action. The Letter of Intent states that per Chapter 8-4 of SECNAV Manual-5510.30, any “interim” or “temporary” access must be immediately removed. The individual may provide a response to DON CAF to mitigate the disqualifying factors. DON CAF will consider the individual's response. If an unfavorable determination is still made after considering the mitigating factors, DON CAF will issue the Letter of Notification to deny eligibility.

¹⁵ The DON CAF Letter of Notification is issued to every individual for whom an unfavorable eligibility determination has been made after consideration of the individual's response to the Letter of Intent. The Letter of Notification states, “You must terminate the individual's access to classified information and/or assignment to sensitive duties, and debrief immediately if the individual is currently indoctrinated for Sensitive Compartmented Information access.

¹⁶ Both the Letter of Notification and Letter of Intent require that an individual's access to classified information be terminated upon DON CAF denial of eligibility.

the command must remove all accesses authorized *and debrief the individual* [emphasis added]...”

- The Letter of Notification states that a debrief is required “immediately [upon denial] if the individual is currently indoctrinated for Sensitive Compartmented Information (SCI) access.” In contrast, the Manual does not limit the debrief requirement to Sensitive Compartmented Information access.

DON Security Managers Did Not Know Actions Required Upon DON CAF Denial. There were no requirements for annual refresher training, certification, or continuing professional education requirements for DON security managers. In addition, only 5 of 11 (45 percent) respondents to our questionnaire indicated they had completed NCIS’s formal required course and only 5 of 11 (45 percent) respondents could sufficiently explain the process after DON CAF denial.

By not having a process in place that ensures the immediate debriefing of individuals denied a security clearance, DON is at risk of allowing unauthorized access to classified information. This creates an unnecessary risk to national security, which can result in significant human loss and financial cost. This is inconsistent with the objective of the DON Personnel Security Program and is in violation of SECNAV M-5510.30.

Recommendations and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses are presented below. The complete text of the management responses is in the Appendix.

We recommend that Director, Naval Criminal Investigative Service:

Recommendation 6. Revise Secretary of the Navy Manual 5510.30 to require a written record be provided to a central oversight authority for each interim access granted. The record should include the individual’s current Department of the Navy command, security manager, supervisor, and the types of information the individual will have access to. If the individual is mobilized or transferred, or if the security manager changes, the record should be updated to reflect the new information. The record should be maintained as a permanent part of the individual’s investigation and adjudication file.

Management response to recommendation 6. Concur. Open. Near-term, N09N2 will develop and staff an interim Department of the Navy policy change providing clarification of memo type and point of retention. Long-term action will require the Secretary of the Navy Manual to be revised and issued. The policy change will identify the Echelon II as the central authority.

Echelon IIs will be required to have subordinate commands submit reports as changes occur, but not less than annually. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 7. Revise Secretary of the Navy Manual 5510.30 to require that within 1 work day following receipt of a Department of the Navy Central Adjudication Facility clearance denial, security managers notify a central oversight authority that debriefs have occurred and access to classified information has been denied.

Management response to recommendation 7. Concur. Open. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires the Secretary of the Navy Manual to be revised and issued. The policy change will specify a specific time frame for security managers to notify and debrief the individual and document the action in the Joint Personnel Adjudication System. Security managers are expected to accomplish these tasks within 5 duty days of receipt of the notification. Notify commander action complete within 1 day. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 8. Revise Secretary of the Navy Manual 5510.30 to require central oversight authority verification that debriefs occurred within the 1-day requirement.

Management response to recommendation 8. Concur. Open. Near-term action: N09N2 to develop and staff an interim Department of the Navy policy change. Long-term action requires the Secretary of the Navy Manual to be revised and issued. This action will be carried out by N09N2 through the use of an automated Joint Personnel Adjudication System report. Report to be reviewed to ensure compliance. At a minimum, this will be accomplished annually, more frequently if anomalies are identified. The target completion date for the actions is 1 March 2012. Management will provide an interim status report on 1 June 2011.

Recommendation 9. Revise the Department of the Navy Central Adjudication Facility Letter of Notification and Letter of Intent to ensure both are consistent with and state the Secretary of the Navy Manual 5510.30 requirement to debrief interim denials immediately.

Management response to recommendation 9. Concur. Open. N09N2 will work with the Department of the Navy Central Adjudication Facility to ensure the Letter of Notification and Letter of Intent are consistent with the Secretary

of the Navy Manual 5510.30. The target completion date for the actions is 1 June 2011.

Naval Audit Service comment on the response to Recommendations 6-9. Actions planned by the Naval Criminal Investigative Service satisfy the intent of the recommendations, which are considered open pending completion of the actions. Regarding the responses to Recommendations 7 and 8, we understand that it may take up to 5 days to complete the entire notification and debrief process, and there may be occasions when debriefing cannot be done within 1 day (e.g., because the subject is not available). However, debriefing should take place as soon as possible during the 5-day timeframe, and, to the maximum extent possible, within 1 day. Also, the planned action to have security managers document the debrief in the Joint Personnel Adjudication System, and notify the commander that action is complete within 1 day, should provide visibility of the action, and meets the intent of notifying a central oversight authority that the debrief has occurred.

Section B:

Status of Recommendations

Recommendations							
Finding ¹⁷	Rec. No.	Page No.	Subject	Status ¹⁸	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁹
1	1	7	Establish oversight policies and procedures for monitoring, inspecting, and reporting on the status/granting of interim accesses for the Department of the Navy, and revise Secretary of the Navy Manual 5510.30 accordingly.	O	Office of the Director, Naval Criminal Investigative Service (NCIS)	3/1/12	6/1/11
1	2	8	Revise Secretary of the Navy Manual 5510.30 to require commanding officers or designated security managers to review and certify, in writing, that no adverse information exists on the Standard Form 86 prior to granting interim access to classified information, with memorandum being retained at the command for higher-level review or inspection as required.	O	Office of the Director, NCIS	3/1/12	6/1/11
1	3	8	Develop mandatory security manager training addressing Secretary of the Navy Manual 5510.30 requirements and responsibilities, and ensure all new security managers promptly complete this training prior to granting an interim clearance.	O	Office of the Director, NCIS	3/1/12	6/1/11
1	4	8	Revise Secretary of the Navy Manual 5510.30 to require security managers to take annual training, and provide documentation of course completion to a central oversight authority.	O	Office of the Director, NCIS	3/1/12	6/1/11

¹⁷ / + = Indicates repeat finding.

¹⁸ / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.

¹⁹ If applicable.

Recommendations							
Finding ¹⁷	Rec. No.	Page No.	Subject	Status ¹⁸	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁹
1	5	9	Issue a "personal for" (P4) message to all commanding officers and security managers emphasizing that Secretary of the Navy Manual 5510.30 only permits the granting of interim access to classified information in the absence of adverse information disclosed on an SF 86. The P4 should also note the new certification, reporting, and training documentation requirements. In addition, the P4 message should address the Secretary of the Navy Manual 5510.30 requirements for the security managers to take the Naval Security Manager Course offered by the Naval Criminal Investigative Service.	O	Office of the Director, NCIS	6/1/11	
2	6	11	Revise Secretary of the Navy Manual 5510.30 to require a written record be provided to a central oversight authority for each interim access granted. The record should include the individual's current Department of the Navy command, security manager, supervisor, and the types of information the individual will have access to. If the individual is mobilized or transferred, or if the security manager changes, the record should be updated to reflect the new information. The record should be maintained as a permanent part of the individual's investigation and adjudication file.	O	Office of the Director, NCIS	3/1/12	6/1/11
2	7	12	Revise Secretary of the Navy Manual 5510.30 to require that within 1 work day following receipt of a Department of the Navy Central Adjudication Facility clearance denial, security managers notify a central oversight authority that debriefs have occurred and access to classified information has been denied.	O	Office of the Director, NCIS	3/1/12	6/1/11
2	8	12	Revise Secretary of the Navy Manual 5510.30 to require central oversight authority verification that debriefs occurred within the 1-day requirement.	O	Office of the Director, NCIS	3/1/12	6/1/11

Recommendations							
Finding ¹⁷	Rec. No.	Page No.	Subject	Status ¹⁸	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁹
2	9	12	Revise the Department of the Navy Central Adjudication Facility Letter of Notification and Letter of Intent to ensure both are consistent with and state the Secretary of the Navy Manual 5510.30 requirement to debrief interim denials immediately.	O	Office of the Director, NCIS	6/1/11	

Exhibit A:

Scope and Methodology

We conducted our review of interim clearances with subsequent Department of the Navy Central Adjudication Facility (DON CAF) denials from 10 November 2009 through 25 January 2011. We visited or contacted officials at each location identified in Exhibit B.

Audit Universe

To identify our universe of interim denials, we queried the DON Joint Personnel Adjudication System (JPAS) data base records extract obtained from the Defense Security Service. Additionally, we matched the data base extract with a separate list of 2009 DON CAF denials. We considered the information obtained through this process as sufficiently reliable for the purposes of our audit of selected interim denials. We did not perform additional tests to validate JPAS since it was beyond the scope of our audit. Our universe consisted of 340 DON-wide interim clearances with DON CAF denial records in JPAS as of 21 January 2010.

Audit Sampling

To obtain an understanding of internal controls over the timely debrief upon DON CAF denial, we queried the entire JPAS data base to review all 340 records by comparing the indoctrination date,²⁰ denial date,²¹ and debrief date.²²

To obtain an understanding of internal controls over the granting of temporary interim security clearances, we used a combination of judgmental and statistical sampling methods to review 42 (12 percent) of the 340 records. Our risk-based judgmental sample included 22 of 143 records of personnel who were never debriefed or debriefed late. Specifically, we selected 11 of 83 records who were never debriefed and 11 of 60 records who were debriefed late. We judgmentally selected records for review based on reason for denial and greatest number of days from DON CAF denial.

We sent questionnaires to the individuals' adjudicators to determine where the adverse information was first disclosed, and if the command was aware of the adverse information prior to granting the interim access. Additionally, we obtained copies of sampled individuals' Standard Forms (SFs) 86 and Office of Personnel Management investigation files to determine whether adverse information was disclosed by the individual on the SFs 86. We attempted to contact the individuals' security managers to

²⁰ Indoctrinate within JPAS means they are assigned an access level. Once a person is indoctrinated at an access level, they will remain at that level until they are debriefed.

²¹ Denial date is the date that DON CAF has determined the person is ineligible to have access to classified information.

²² Debrief within JPAS means the person's level of access has been removed.

determine whether the individuals were still employed by DON and what levels of classified information the individuals had access to, both prior to and following the denial. Further, we sent a written questionnaire to the same security managers to determine their training and awareness regarding what procedures they should follow after DON CAF denial. We summarized the results for reporting purposes in a Microsoft Excel spreadsheet.

To determine whether similar results relating to adverse information disclosed on the SFs 86 existed in those 197 records of personnel who were debriefed on time, we used a statistical sample of 20 of the 197 records showing debriefs that occurred on time. We received documentation for 18 of the 20 sampled records. Of these 18 records, we identified 15 with adverse information on the SFs 86. Given these sample results, we can project with 90 percent confidence that at least 110 out of 197 records had adverse information on their SFs 86.

We reviewed compliance with applicable laws and regulations relating to the personnel security program. We contacted numerous activity personnel, including the Naval Criminal Investigative Service, DON CAF, the Defense Manpower Data Center, and the Defense Security Service.

We did not identify any audit reports within the past 5 years on the DON personnel security clearance process, so no follow up was necessary.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Exhibit B:

Activities Visited and/or Contacted

- Bureau of Medicine and Surgery, Washington, DC
- Bureau of Naval Personnel, Millington, TN
- Chief of Naval Operations, Washington, DC
- Commandant of the Marine Corps, Washington, DC
- Defense Security Service, Alexandria, VA*
- Defense Manpower Data Center, Seaside, CA
- Department of the Navy Central Adjudication Facility, Washington, DC*
- Military Sealift Command, Washington Navy Yard, DC
- Naval Air Systems Command, Patuxent River, MD
- Naval Criminal Investigative Service, Washington, DC*
- Naval Education and Training Command, Pensacola, FL
- Naval Facilities Engineering Command, Washington, DC
- Naval Inspector General, Washington, DC
- Naval Reserve Forces Command, New Orleans, LA
- Naval Sea Systems Command, Washington, DC
- Naval Supply Systems Command, Mechanicsburg, PA
- Navy Installations Command, Washington, DC
- Navy Recruiting Command, Millington, TN
- Space and Naval Warfare Systems Center, Charleston, SC
- U.S. Fleet Forces Command, Norfolk, VA
- U.S. Pacific Fleet, Pearl Harbor, HI

*Activities Visited

Appendix:

Management Response from Director, Naval Criminal Investigative Service



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

5513
Ser N09N2/11U213036

MAR 04 2011

MEMORANDUM FOR ASSISTANT AUDITOR GENERAL FOR MANPOWER AND
RESERVE AFFAIRS, AUDITS

SUBJECT: NAVAUDSVC Draft Audit Report N2009-NFO000-0056

I am responding to your letter of January 25, 2011 to review the findings and recommendations contained in the draft audit report "Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Selected Activities."

I concur with the report as written and our responses to the findings and recommendations are contained in Attachment A.

The Department of the Navy point of contact for this audit is [REDACTED]
can be reached at [REDACTED]

FOIA (b)(6)

[REDACTED]

FOIA (b)(6)

Special Assistant for Naval Investigative
Matters and Security

Attachments:
As stated

Copy to:
Audit Director

Naval Audit Service Report N2009-NFO000-0056 Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Select Activities Recommendations							
Findings	Rec. No.	Page No.	Subject	Status	Action Command	Target or Actual Completion Date	Interim Target Completion Date
1	1	7	Establish oversight policies and procedures for monitoring, inspecting, and reporting on the status/granting of interim accesses for the Department of the Navy, and revise Secretary of the Navy Manual-5510.30 accordingly.	Concur - Open - Near term action N09N2 to develop and staff an interim DON policy change. Long term action requires SECNAV Manual to be revised and issued.	DIRNCIS	3/1/2012	6/1/2011
1	2	7	Revise Secretary of the Navy Manual-5510.30 to require commanding officers or designated security managers to review and certify, in writing, that no adverse information exists on the Standard Form 86 prior to granting interim access to classified information, with memorandum being retained at the command for higher-level review or inspection as required.	Concur - Open - Near term action N09N2 to develop and staff an interim DON policy change. Long term action requires SECNAV Manual to be revised and issued.	DIRNCIS	3/1/2012	6/1/2011
1	3	7	Develop mandatory security manager training addressing Secretary of the Navy Manual-5510.30 requirements and responsibilities, and ensure all new security managers promptly complete this training prior to granting an interim clearance.	Concur - Open - N09N2 will determine best method of ensuring the security managers accomplish required training. Near term action N09N2 to develop and staff an interim DON policy change. Long term action requires SECNAV Manual to be revised and issued. The policy change will include specific training requirements that need to be accomplished within 30 days of assumption of security manager duties. Preferred method is to use the Defense Security Service's existing on-line training resources to track and monitor completion of the requirements.	DIRNCIS	3/1/2012	6/1/2011

Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Select Activities Recommendations						
Naval Audit Service Report N2009-NFO000-0056						
Findings	Rec. No.	Page No.	Subject	Status	Action Command	Target or Actual Completion Date
1	4	8	Revise Secretary of the Navy Manual-5510.30 to require security managers to take annual training, and provide documentation of course completion to a central oversight authority.	Concur - Open - N09N2 will identify annual training requirements for security managers and determine best method of ensuring the training is accomplished and documented. Near term action N09N2 to develop and staff an interim DoN policy change. Long term action requires SECNAV Manual to be revised and issued.	DIRNCIS	3/1/2012
1	5	8	Issue a "personal for" (P4) message to all commanding officers and security managers emphasizing that Secretary of the Navy Manual-5510.30 only permits the granting of interim access to classified information in the absence of adverse information disclosed on an SF 86. The P4 should also note the new certification, reporting, and training documentation requirements. In addition, the P4 message should address the Secretary of the Navy Manual-5510.30 requirements for the security managers to take the Naval Security Manager Course offered by the Naval Criminal Investigative Service	Concur - Open- N09N2 will draft and staff a suggested memorandum for the N09N. The P4 will remind commanders of the requirement to review the SF86 information prior to issuing an interim security clearance. It will also remind commanders of the requirement for Security Managers to attend suitable training.	DIRNCIS	6/1/2011

Naval Audit Service Report N2009-NFO000-0056 Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Select Activities Recommendations							
Findings	Rec. No.	Page No.	Subject	Status	Action Command	Target or Actual Completion Date	Interim Target Completion Date
2	6	10	Revise Secretary of the Navy Manual-5510.30 to require a written record be provided to a central oversight authority for each interim access granted. The record should include the individual's current Department of the Navy command, security manager, supervisor, and the types of information the individual will have access to. If the individual is mobilized or transferred, or if the security manager changes, the record should be updated to reflect the new information. The record should be maintained as a permanent part of the individual's investigation and adjudication file.	Concur - Open - Near term N09N2 will develop and staff an interim DON policy change providing clarification of memo type and point of retention. Long term action will require SECNAV Manual be revised and issued. The policy change will identify the Echelon II as the central authority. Echelon IIs will be required to have subordinate commands submit reports as changes occur, but not less than annually.	DIRNCIS	3/1/2012	6/1/2011
2	7	10	Revise Secretary of the Navy Manual-5510.30 to require that within 1 work day following receipt of a Department of the Navy Central Adjudication Facility clearance denial, security managers notify a central oversight authority that debriefs have occurred and access to classified information has been denied.	Concur - Open - Near term action N09N2 to develop and staff an interim DON policy change. Long term action requires SECNAV Manual to be revised and issued. The policy change will specify a specific time frame for security managers to notify and debrief the individual and document the action in JPAS. Security Managers are expected to accomplish these tasks within 5 duty days of receipt of the notification. Notify commander action complete within 1 day.	DIRNCIS	3/1/2012	6/1/2011

Naval Audit Service Report N2009-NFO000-0056 Effectiveness of the Department of the Navy's Denial Process for Interim Security Clearances at Select Activities Recommendations						
Findings	Rec. No.	Page No.	Subject	Status	Action Command	Interim Target Completion Date
2	8	11	Revise Secretary of the Navy Manual-5510.30 to require central oversight authority verification that debriefs occurred within the 1-day requirement.	Concur - Open - Near term action N09N2 to develop and staff an interim DON policy change. Long term action requires SECNAV Manual to be revised and issued. This action will be carried out by N09N2 through the use of an automated JPAS report. Report to be reviewed to ensure compliance. At a minimum this will be accomplished annually, more frequently if anomalies are identified.	DIRNCIS	3/1/2012
2	9	11	Revise the Department of the Navy Central Adjudication Facility Letter of Notification and Letter of Intent to ensure both are consistent with and state the Secretary of the Navy Manual-5510.30 requirement to debrief interim denials immediately.	Concur - Open - N09N2 will work with the DONCAF to ensure the Letter of Notification and Letter of Intent are consistent with the SECNAV Manual 5510.30.	DIRNCIS	6/1/2011

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies

of this document

~~FOR OFFICIAL USE ONLY~~