

Naval Audit Service



Audit Report



Navy Antiterrorism Program Execution

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

*Releasable outside the Department of the Navy
only on approval of the Auditor General of the Navy*

N2009-0004
22 October 2008

Obtaining Additional Copies

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

Phone: (202) 433-5757
Fax: (202) 433-5921
Email: 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
Email: 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>



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

7510
N2008-NIA000-0051.000
22 Oct 08

MEMORANDUM FOR CHIEF OF NAVAL OPERATIONS (N3AT, N46)

Subj: **NAVY ANTITERRORISM PROGRAM EXECUTION**
(AUDIT REPORT N2009-0004)

Ref: (a) NAVAUDSVC memo 7540 N2008-NIA00-0051.000, dated 27 September 2007
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

1. The report provides our 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 Appendices.
2. The Office of the Chief of Naval Operations (CNO) (N3AT) responded to Recommendation 1, and CNO (N46) responded to Recommendations 2-9. CNO (N3AT) and CNO (N6) concurred with the recommendations, which are open pending completion of agreed-to actions. Summaries of the management responses, and our comments, are in the finding; the full text of the management responses is in the Appendices. The open recommendations are subject to monitoring in accordance with reference (b). Management should provide a written status report on the recommendations within 30 days after each target completion date.
3. Please provide all correspondence to the Assistant Auditor General for Installations and Environment Audits [REDACTED], with a copy to the Director, Policy and Oversight, [REDACTED]. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.
4. 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: **NAVY ANTITERRORISM PROGRAM EXECUTION**
(AUDIT REPORT N2009-0004)

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



Assistant Auditor General
Installations and Environment Audits

Copy to:
UNSECNAV
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV IE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N4B, N40)
CMC (RFR, ACMC)
DON CIO
NAVINGEN (NAVIG-4)
USFFC
AFAA/DO

Table of Contents

EXECUTIVE SUMMARY	4
SECTION A: FINDING AND RECOMMENDATIONS.....	1
Finding 1: Navy Antiterrorism Strategic Plan	1
Synopsis.....	1
Discussion of Details.....	2
Background	2
Audit Results	3
Antiterrorism Strategic Plan Reporting Responsibilities, Oversight, and Verification	4
Compliance With AT Strategic Plan Sub-Objectives	5
AT Plans	7
Antiterrorism Strategic Plan Reporting Tools.....	11
Antiterrorism Readiness Management System (ARMS)	12
Commander, Pacific Fleet (COMPACFLT) Tracking System	13
CVAMP.....	13
DRRS-N	13
Vulnerabilities Analysis	14
Lack of POA&M Guidance.....	15
POA&M Best Business Practices	16
POA&M Analysis	17
Adequate POA&Ms	18
Inadequate POA&Ms	18
Risk Acceptance	19
Conclusion.....	20
Recommendations	20
SECTION B: STATUS OF RECOMMENDATIONS.....	25
EXHIBIT A: BACKGROUND.....	26
EXHIBIT B: SCOPE AND METHODOLOGY.....	27
Scope	27
Methodology.....	27
EXHIBIT C: ACTIVITIES VISITED AND/OR CONTACTED	29
EXHIBIT D: PERTINENT GUIDANCE	30
EXHIBIT E: LIST OF ACRONYMS.....	32
APPENDIX 1: MANAGEMENT RESPONSE FROM OFFICE OF THE CHIEF OF NAVAL OPERATIONS (N3AT)	34
APPENDIX 2: MANAGEMENT RESPONSE FROM OFFICE OF THE CHIEF OF NAVAL OPERATIONS (N46)	37

Executive Summary

Objective

Verify that Navy installation vulnerabilities and achievement of Antiterrorism (AT) Strategic Plan goals and objectives are being recorded, tracked, and reported; and management of AT execution is in accordance with applicable Department of Defense (DoD) and Navy policies and guidance.

Overview

The AT Strategic Plan outlines a results-oriented management framework that guides the DoD Components toward effective, proactive, and viable AT Programs. To accomplish that objective, DoD and Navy AT Strategic Plans specifically outline 5 goals and 35 sub-objectives that represent essential elements of an AT Program that, if met, reduce the Navy's vulnerabilities to terrorist acts.

Installations are required to implement an AT risk management strategy that includes threat, criticality, vulnerability, and risk assessments. In order to employ an effective risk management strategy, all vulnerabilities identified in a vulnerability assessment must be clearly listed, tracked, and validated. According to DoD guidelines, all AT vulnerability assessment data must be entered into the Core Vulnerability Assessment Management Program (CVAMP) database. Also, Plans of Actions and Milestones (POA&Ms) are an effective tool for use in tracking, managing, and mitigating identified vulnerabilities.

We determined that all 6 Navy Continental United States (CONUS) regions were submitting the status of their installations in complying with AT Strategic Plan sub-objectives and associated DoD/Navy AT Standards; however the Navy has not established a process to verify installation compliance. As a result, we identified discrepancies between the reported and actual levels of compliance.

Additionally, we found that (per DoD guidance) CVAMP had generally been populated with some of the identified vulnerabilities at the majority of the 22 Navy installations audited. However, 32 percent of identified vulnerabilities within our sample had not been entered. DoD requires development of mitigation actions for all identified vulnerabilities. However, DoD guidance does not mandate that mitigation actions (POA&Ms) be entered into CVAMP. We determined that more than 40 percent of vulnerabilities identified within our sample did not have an associated POA&M entered into CVAMP.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act (FMFIA) 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. In our opinion, the conditions noted in this report may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

Noteworthy Accomplishments

Commander, Navy Region Southeast (CNRSE), has internally funded the development and implementation of the Antiterrorism Readiness Management System which provides the region with the added capability of recording, tracking, and reporting of risk management information, and event and exercise approval, and can also serve as an AT guidance library.

Four regions employ a CVAMP coordinator to monitor CVAMP compliance.

The Commanders, Navy Region Northwest and Navy Region Southwest, have internally funded Antiterrorism Officer positions at selected installations, thereby providing stability and continuity within installation AT Programs.

Commander, Navy Installations Command (CNIC), in conjunction with the Naval Facilities Engineering Service Center, has developed and begun deploying Risk-Analyzed Mitigation Process teams to assist installation commanders and AT staff in identifying and developing Mitigation Action Plans to mitigate identified vulnerabilities, as well as assess CVAMP entries for correctness and completeness.

Recommendations

Office of the Chief of Naval Operations (CNO (N3AT)):

Develop procedures establishing CNO (N3AT)'s involvement in the AT Strategic Plan reporting process to ensure sufficient visibility to aid in making both AT-related procedural (requirements/manpower) and programmatic (funding) decisions.

CNO (N46):

Develop controls (in the form of a web-based tracking system) and implement guidance to ensure that regional commands provide oversight by validating installation-level compliance with DoD/Navy AT standards and associated AT Strategic Plan sub-objectives.

Establish the required frequency of installation Antiterrorism Working Group meetings; clarify and document in guidance to ensure the requirement is consistently followed by installations.

Develop an annual AT program review tool and clarify guidance mandating its use at both the regional and installation level.

Clarify guidance regarding use of the Joint Antiterrorism (JAT) guide to develop installation AT Plans and conduct required annual AT assessments and AT Plan reviews. Further, develop an implementation plan to ensure that all CONUS Navy Installation AT personnel have access to the JAT guide.

Develop controls and provide oversight to ensure that current guidance regarding CVAMP responsibilities at both the regional and installation level are adhered to, ensuring that identified vulnerabilities are entered within CVAMP, and that installation-level AT-related assessments are properly performed, documented, and retained in official files.

Develop an implementation plan to ensure that all CONUS Navy installations have dedicated and reliable Secured Internet Protocol Router Network access to facilitate use of CVAMP.

Develop controls, implement guidance, and provide oversight to ensure that AT personnel develop (and enter into CVAMP) effective POA&Ms for tracking, reporting, and mitigating or eliminating vulnerabilities per Department of Defense Instruction 2000.16.

Develop guidance defining the minimum required elements to be included within POA&Ms.

Corrective Actions

The Office of the Chief of Naval Operations (CNO) (N3AT) responded to Recommendation 1, and CNO (N46) responded to Recommendations 2-9. CNO (N3AT) and CNO (N6) concurred with the recommendations, which are open pending completion of agreed-to actions.

Section A:

Finding and Recommendations

Finding 1: Navy Antiterrorism Strategic Plan

Synopsis

The Navy's Antiterrorism (AT) policy component (Office of the Chief of Naval Operations (CNO) (N3AT))¹ and resourcing component (Commander, Navy Installations Command (CNIC)) do not currently have visibility of the results of the annual AT Strategic Plan submissions to the Office of the Secretary of Defense (OSD). We identified significant inaccuracies within quarterly Continental United States (CONUS) Navy regional reports to United States Fleet Forces Command (USFFC) regarding installation compliance with sub-objectives outlined within the Department of Defense (DoD) AT Strategic Plan. We also learned that Navy CONUS installations audited had not consistently entered all identified vulnerabilities into the Core Vulnerabilities Assessment Management Program (CVAMP) system per DoD guidance, nor had corresponding Plans of Action and Milestones (POA&Ms) for each vulnerability been consistently developed and entered into CVAMP.

DoD AT Strategic Plan reporting inaccuracies occurred because no official verification, oversight, and tracking process had been established to ensure the validity of installation-level compliance with AT Strategic Plan sub-objectives. Most CONUS Navy regions did not have adequate controls in place to verify that AT Strategic Plan goals and sub-objectives were being met at CONUS Navy installations. CVAMP-compliance issues occurred because of: (1) a lack of CVAMP access due to unreliable/unavailable Secure Internet Protocol Router Network (SIPRNET) connectivity; (2) a lack of clear guidance regarding POA&M implementation expectations or requirements; and (3) a lack of guidance regarding what is to be included within an effective and robust POA&M.

DoD AT Strategic Plan compliance reporting inaccuracies: As a result of the lack of visibility and verification, higher-level commands may not have a complete and accurate view of the Navy's ability to meet the requirements outlined in the DoD/Navy AT Strategic Plan. Therefore, higher headquarters (HHQs) cannot effectively assess the status of the Navy shore installation AT Program. Without visibility, AT areas that need improvement may not receive sufficient management attention and/or needed resources.

¹ As of June 2008, CNO N46 was assigned primary responsibility for Continental U.S. (CONUS) Ashore Antiterrorism policy, and will remain the ASHORE resource sponsor, controlling both primary policy and funding decisions regarding the Navy's CONUS ASHORE AT Program. CNO (N3AT) will retain strategic oversight of Navy AT policy.

Further, the Office of the Secretary of Defense (OSD) may be receiving an inaccurate annual assessment regarding the status of Navy installations in meeting DoD AT standards.

CVAMP compliance: Without CVAMP being fully populated with identified vulnerabilities and associated POA&Ms, HHQs may not have sufficient visibility and/or information for making priority and funding decisions, which could result in identified vulnerabilities not receiving sufficient management attention or needed resources.

Discussion of Details

Background

The Global War on Terrorism (GWOT) requires increased levels of diligence, awareness, and protection throughout the armed services. Following the terrorist attack on the USS *Cole* in 2000, Congress and DoD evaluated their AT programs and diagnosed gaps within the current program that needed to be mitigated. DoD AT Program guidance (DoD Directive 2000.12) and the DoD AT Standards (DoD Instruction 2000.16) were revised as a result of this evaluation.

The Government Accountability Office (GAO), in a September 2001 report (GAO-01-909), recommended that the Secretary of Defense direct the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (OASD (SO/LIC)) to establish a management framework for the antiterrorism program that would provide the department with a vehicle to guide resource allocations and measure the results of improvement efforts. It is noted that a strategic plan and a supporting implementation plan should be developed that clearly describes and defines:

- Long-term antiterrorism goals;
- Performance goals that are objective, quantifiable, and measurable;
- Performance indicators to measure outputs; and
- An evaluation plan to compare program results to established goals.

In 2002-2003, in conjunction with this GAO report, and following the terrorist attack on September 11, 2001, Congress, along with the Assistant Secretary of Defense for Homeland Defense (ASD/HD), requested another evaluation to address the effectiveness of the then-current AT standards that had been in place since 1983. As a result, ASD/HD drafted for SO/LIC the DoD Antiterrorism Strategic Plan, DoD O-2000.12-P, to outline a results-oriented management framework that guides the DoD Components toward effective, proactive, and viable AT Programs. It identifies 5 strategic goals, 35 sub-objectives, and a proposed strategy for achievement.

In 2005, CNO (N3AT) developed the Navy AT Strategic Plan (Office of the Chief of Naval Operations (OPNAV) Instruction 3300.56) as directed by DoD O-2000.12-P. Both OPNAVINST 3300.56 (“Navy AT Strategic Plan”) and OPNAVINST 3300.53B (“Navy AT Program”) designate CNO (N3AT) as the responsible agent for managing the Navy’s AT Strategic Plan. USFFC is designated as the Navy’s Executive Agent for AT in OPNAV Instruction 3300.53B. With this designation, USFFC is responsible for reporting annually to U.S. Northern Command (USNORTHCOM) the status and the progress of Navy installations in the six CONUS regions in achieving the strategic goals and performance objectives described in DoD O-2000.12-P.

DoD Directive 2000.12 requires the Navy to maintain a centralized database of all vulnerability assessments. DoD Instruction (DoDI) 2000.16 mandates that CVAMP be populated with all vulnerability assessment results, and that mitigation plans are developed to mitigate or eliminate the potential impact of identified vulnerabilities. In a memo dated 25 May 2005, the Department of the Navy (DON) mandated the use and maintenance of CVAMP to track all actions planned and/or taken to mitigate AT vulnerabilities.

Pertinent Guidance

See Exhibit D.

Audit Results

The DoD AT Strategic Plan (DoD O-2000.12P) outlines a results-oriented management framework that guides DoD Components toward effective, proactive, and viable AT Programs. It identifies 5 strategic goals, 35 sub-objectives based on DoD AT Standards, and a proposed strategy for achievement. We audited 15 of the 35 sub-objectives and found discrepancies in reported compliance levels.

Our audit showed that all six CONUS Navy regions are currently submitting quarterly AT Strategic Plan results to USFFC as required; however, we identified opportunities to improve the verification and validation, visibility, tracking, and reporting of installation compliance with current DoD and Navy AT standards through the chain of command.

Throughout the audit potential action commands were kept abreast of audit results and potential recommendations via periodic phone conversations and briefings, as meetings were held with CNO (N3AT) (March 2008) and CNO (N46) (August 2008) AT officials. Additionally we provided point papers to each of the six regions audited at the conclusion of each of the site visits detailing noteworthy accomplishments and areas of concern at both the regional and installation level.

Antiterrorism Strategic Plan Reporting Responsibilities, Oversight, and Verification

OPNAV Instruction 3300.56 and 3300.53B, states that CNO (N3AT) is responsible for managing the Navy's AT Strategic Plan. However, we determined that CNO (N3AT) has no direct visibility and/or participation in the annual AT Strategic Plan reporting process. A Joint Staff memorandum dated 6 September 2007 noted that reporting from military departments was not required for the Fiscal Year 2007 Strategic Plan review. However, the memorandum further stated that the lack of direct reporting from the services (Navy, CNO (N3AT)) to the Joint Staff does not alleviate the service requirement to have and implement an AT Strategic Plan with performance and compliance measures. We also found that a process to verify and validate installation-level AT Strategic Plan compliance results had not been developed or mandated by CNO (N3AT), CNIC, and USFFC. As a result, CNO (N3AT), CNIC, and USFFC have limited assurance of the accuracy and validity of the Navy's reported level of compliance with each of the 35 sub-objectives outlined in the DoD/Navy AT Strategic Plans.

OSD officials noted that they are required to track and report to Congress the status regarding compliance with the 35 sub-objectives of the DoD AT Strategic Plan by each Combatant Command (COCOM) and their subordinate regions within their area of responsibility. According to a Joint Staff memorandum, USNORTHCOM was tasked with the responsibility of reporting CONUS military installations' progress toward achieving AT Strategic Plan performance objectives to OSD, in accordance with the USNORTHCOM AT Strategic Plan.

To help fulfill their reporting responsibility to OSD, USNORTHCOM developed an AT Strategic Plan reporting template, and in 2005 mandated its use by its subordinate commands. USFFC, the Navy's AT Executive Agent to USNORTHCOM, tasked the six CONUS regions with compiling installation-based AT Strategic Plan compliance reports, and submitting them to USFFC. USFFC would then provide a comprehensive AT Strategic Plan report to USNORTHCOM for eventual annual submission to OSD. However, USFFC officials noted that they do not verify, validate, or test the accuracy of the quarterly submissions received from the regions. Instead, USFFC relies on regional AT personnel to verify quarterly installation submission results, and accurately report compliance with AT Strategic Plan sub-objectives.

As of March 2007, USNORTHCOM no longer requires USFFC to submit quarterly AT Strategic Plan compliance reports. However, USNORTHCOM officials noted that they continue to report the Navy's annual compliance to OSD based, in part, on the success of previous USFFC AT program reviews conducted by USNORTHCOM, which were focused only on USFFC and not on individual regions' or installations' compliance. We obtained the 2007 OSD annual AT Strategic Plan compliance report. In this report, the

USNORTHCOM data showed that all 4 services had achieved satisfactory levels of compliance (92-100 percent) for all 15 AT Strategic Plan sub-objectives within our audit scope. However, our review (addressed in the following section) identifies several significant discrepancies with the USNORTHCOM data.

USFFC officials also noted that they rely on the Defense Readiness Reporting System/Navy (DRRS-N) system to report compliance with DoD/Navy AT Standards and associated AT Strategic Plan sub-objectives. As a result, they believe the current quarterly reporting process is no longer necessary. However, we found that DRRS-N does not currently address any of the 35 sub-objectives of the AT Strategic Plan and, therefore, does not allow for verification and validation of reported levels of compliance. If modified to include each of the AT Strategic Plan sub-objectives, however, DRRS-N could potentially be used in this capacity. If DRRS-N is not modified or a tracking system is not put in place, AT Program weaknesses may not receive sufficient management and HHQ attention and funding.

We determined that regional AT departments and programs did not have an effective process in place to verify or validate the accuracy of installation-level compliance with AT Strategic Plan sub-objectives to facilitate quarterly reporting to USFFC using the USNORTHCOM-mandated reporting template. Some regional officials attempted to verify the status of installation compliance based on periodic communication via emails and/or phone calls with installation AT personnel. However, these regions were not consistently requesting, receiving, or viewing supporting documentation from the installations.

We concluded that the Navy lacked an adequate tracking and control system over the entire AT Strategic Plan reporting process, including compliance with individual sub-objectives and associated DoD/Navy AT Standards.

Compliance With AT Strategic Plan Sub-Objectives

The AT program elements discussed in DoD guidance are fully outlined in the AT Strategic Plan as 5 goals and 35 sub-objectives that have been designed to assist installations in the development of an effective AT program. According to OSD officials the DoD AT Strategic Plan was originally planned to be phased out by 2011 as all sub-objectives were scheduled to be achieved; however we learned that OSD is currently in the process of revising the DoD AT Standards (DoD Instruction 2000.16) to include all of the elements of the AT Strategic Plan, further emphasizing the importance of full compliance with AT Strategic Plan elements.

Our audit scope and analysis focused on 15 of the 35 sub-objectives that we deemed most relevant to achieving a robust and effective installation-level AT Program. These 15, which include elements such as assessments, working groups, AT Plans, and vulnerability tracking and recording, were also areas of concern identified during our

previous AT audits. The remaining 20 sub-objectives were not selected for analysis because they were addressed to COCOMs or dealt with non-installation level issues. Results of our analysis of the 15 sub-objectives were then compared to the current regional AT Strategic Plan reporting results to determine the validity of the information reported through the chain of command, and ultimately to OSD.

The analysis below focuses on the five sub-objectives that showed the largest discrepancy between actual installation compliance levels and the information reported to USFFC by the six Navy regions. As noted above, USFFC had received regional compliance reports but did not forward these results to USNORTHCOM, who ultimately reported compliance levels of 92-100 percent to OSD for all 15 sub-objectives we audited. We found that AT Plans, criticality and risk assessments, as well as required AT-related working groups (Threat Working Group (TWG), Antiterrorism Executive Committee(ATEC)), had not been consistently developed, conducted, accurately reported, or adequately maintained by all installations within our audit scope. The 6 CONUS Navy regions audited submitted compliance reports to USFFC representing the 66 installations within their area of responsibility (AOR) for most of the 35 sub objectives.² Specific installations were not identified on these quarterly compliance reports; therefore, a direct comparison between actual sub-objective compliance by the 22 installations audited and results reported by the regions for all 66 would not be possible.

Our analysis of 2007 fourth quarter³ AT Strategic Plan reports for 22 installations visited showed the following in comparison to what regions reported to USFFC:⁴

- Only 1 of 22 installations (5 percent) within our scope had developed an AT Plan with all required elements in 2007 and AT Plans at an additional 8 installations (36 percent) contained a majority of required elements; CONUS Navy regions reported that 33 of 37 (89 percent) had developed AT Plans with all required elements.
- 12 of 22 installations (55 percent) within our scope had conducted a criticality assessment (CA) in 2007; CONUS Navy regions reported 59 of 66 installations (89 percent) had conducted a CA.

² We found that 5 of the DoD AT Strategic Plan sub-objectives included within the scope of our audit were not included on the quarterly reporting template for 2 of the regions audited resulting in a reduction of 29 installations reported by the 6 regions from 66 to 37 for Vulnerability Assessments, AT Plans, FPCONs, ATO and Staff, and Exercises. This affects the discussion of these 5 sub-objectives below.

³ Fourth quarter, in this instance, does not specifically refer to the period of Oct thru Dec. USNORTHCOM guidance specifies, for the purposes of AT Strategic Plan compliance reports, that the fourth quarter addresses the period of September through November, with a report due date of December 10.

⁴ The quarterly regional AT Strategic Plan reports did not consistently identify specific installations by name. Therefore, a direct comparison of the compliance levels we identified for the 22 installations within our audit scope to the installation compliance levels reported by the regions to USFFC could not be conducted. As a result, there is the potential for the non-complying installations within our scope to be included in the regional compliance results reported to USFFC; however, our analysis identified discrepancies in the reporting process, necessitating increased controls and oversight.

- 11 of 22 installations (50 percent) within our scope had conducted a risk assessment (RA) in 2007; CONUS Navy regions reported 61 of 66 installations (92 percent) had conducted an RA.
- Only 5 of 22 installations (23 percent) within our scope had conducted a TWG during the fourth quarter of 2007; CONUS Navy regions reported 60 of 66 installations (91 percent) had convened TWGs.
- Only 6 of 22 installations (27 percent) within our scope had conducted an ATEC during the second half of 2007; CONUS Navy regions reported 57 of 66 installations (86 percent) had conducted ATECs.

Other Major AT Strategic Plan Elements

We learned that 5 of the 15 sub-objectives included within the scope of our audit were not included on the quarterly reporting template for two of the regions⁵ audited. These two regions are responsible for reporting on a total of 29 installations within their AOR. Therefore, for 5 elements of the AT Strategic Plan, the 6 regions reported compliance levels for only 37 installations instead of 66 as with the other audited AT Strategic Plan sub-objectives. Those 5 absent sub-objectives were: AT Plans; Vulnerability Assessments; Force Protection Conditions (FPCONs); Antiterrorism Officer; and Exercises. A discussion of those five sub-objectives that were not included within two of the six regional compliance reports follows. The other 10 sub-objectives that we audited are addressed in the bullets above, and elsewhere in this finding.

AT Plans

In addition to the analysis of required elements of AT Plans (above), per DoDI 2000.16, AT Plans must be annually reviewed. In addition to the discrepancy regarding the accuracy of reported levels of installation AT Plan compliance, we identified another area for improvement as only 7 of 22 AT Plans had been signed and updated, signifying the completion of an annual review, in 2007.

Vulnerability Assessments (VA)

According to the DoD Instruction 2000.16, a VA is developed to determine the susceptibility and vulnerability to a terrorist attack. Therefore, a VA report detailing identified vulnerabilities to an installation, or a VA matrix specifying the vulnerability to an attack of a specific asset in an installation, are both considered VAs. Also, according to guidance, a Higher Headquarters Assessment (HHA) that follows the Defense Threat

⁵ Both regions reported on the other 10 sub-objectives contained within the scope of our audit.

Reduction Agency (DTRA) Joint Staff Integrated Vulnerability Assessment (JSIVA) guidelines satisfied the intent of a VA for the installation.

We determined that 21 of 22 installations audited (95 percent) had conducted a VA in 2007, as opposed to 30 percent compliance identified in previous AT audits. One installation had not conducted a VA. A review of the 21 installations that had completed a VA for 2007 showed that 13 had an HHA performed (JSIVA/Chief of Naval Operations Integrated Vulnerability Assessment (CNOIVA) or Regional assessment) that satisfied the VA requirement. Additionally, 8 of the 21 installations had conducted a local VA to identify vulnerabilities at the installation.

Site-Specific Force Protection Conditions

OPNAV Instruction 3300.53B requires installations to develop site-specific measures or actions for each FPCON. Regions reported that 36 of 37 installations (97 percent) were complying with this requirement. We found that the installations within our scope had generally developed site-specific FPCONs and were included in the installation's current AT Plan (19 of 22 installations, or 86 percent); or were in the process of updating their AT Plans to include development of site-specific FPCONs.

Antiterrorism Officer (ATO) Level II Trained

CONUS Navy regions reported that 32 of 37 installations (86 percent) had an ATO. We found that all 22 installations had assigned personnel to perform the duties of an ATO to manage the installation AT Program. However, 2 installations were not in compliance with the DoD requirement to have a commissioned officer, non-commissioned officer (E-7 or higher), or civilian staff officer be assigned as the ATO as these installations had assigned ATO duties to Master at Arms (MA1) personnel. Additionally, 12 of 22 installations had dual-hatted personnel performing ATO duties.

Exercises including WMD/CBRNE/FPCON Scenarios

CONUS Navy regions reported that 12 of 37 installations (32 percent) had conducted exercises in 2007 to include Weapon of Mass Destruction and/or Chemical, Biological, Radiological, Nuclear, or High Yield Explosive (WMD/CBRNE) scenarios, and FPCONs exercised through FPCON Delta. In 2007, all 22 installations within our audit scope were required to, and had, participated in Solid Curtain/Citadel Shield, a Navy-wide exercise that included WMD and CBRNE scenarios. However, we learned that 2 of 22 installations did not exercise WMD/CBRNE scenarios per DoD guidance, and 10 had not exercised FPCON measures through Delta. Solid Curtain was designed to exercise only installations' capabilities and response to the increase of FPCONs through FPCON Charlie.

Antiterrorism Working Groups (ATWGs)

In the 2007 fourth quarter AT Strategic Plan submission, regions reported that 61 of 66 installations (92 percent) had conducted an ATWG during the second half of 2007. We found that 17 of 22 installations audited (77 percent) had conducted ATWGs semi-annually as required by DoD and OPNAV guidance. While room for improvement is noted regarding the accurate reporting of installation-level compliance, the 77 percent compliance level that we found represents an improvement over the compliance level identified in the only previous AT audit that had addressed ATWGs (6 of 11 installations, or 55 percent compliance identified within the previous Commander, Navy Region Mid-Atlantic (MIDLANT) AT audit).

For the time period of our review, conflicting guidance existed – and still exists – regarding the required frequency of ATWG meetings. OPNAV Instruction 3300.53A, which was in effect until November 2007, does not specifically state the frequency of such meetings at the installation level. OPNAV Instruction 3300.53B, which was issued in November 2007 and cancels 3300.53A, refers to DoD Instruction 2000.16 that states that ATWGs should be held semi-annually. However, OPNAV Instruction 5530.14D and OPNAV Instruction 3300.56 both indicate that ATWGs should meet at least quarterly. To ensure consistency among installations with regard to ATWG frequency and to make sure that they are complying with the minimum requirements for ATWG meetings, CNO (N3AT) should determine and clearly identify in guidance the required frequency of ATWG meetings.

Threat Assessments (TA)

Regions reported that 61 of 66 installations (92 percent) had conducted TAs. OPNAV Instruction 3300.53B tasks the Naval Criminal Investigative Service (NCIS) with the development of TAs, and tasks installations with requesting TAs from NCIS as well. Since NCIS develops these assessments for every CONUS Navy region, we have determined that this AT Strategic Plan element was completed satisfactorily by the 22 installations within our scope. However, DoD O-2000.12-H states that a TA matrix should be developed by installations on an annual basis. We found that 11 of 22 installations within our scope had not conducted a localized TA matrix in 2007.

Joint Staff Integrated Vulnerability Assessment/Higher Headquarters Assessment

Regions were not required to report on the level of compliance with the requirement to conduct a JSIVA/HHA assessment tri-annually. The reporting template provided by USSFC to the regions did not contain any questions regarding this requirement, even though it is one of the sub-objectives of the DoD AT Strategic Plan. However, we

requested documentation from the installations and found that all 22 installations had conducted a JSIVA or CNOIVA within the last 3 years.

Antiterrorism Program Reviews

DoD Instruction 2000.16 Standard 31 states that comprehensive AT Program Reviews are to be conducted at least annually by all commanders who are required to establish AT programs, in order to evaluate the effectiveness and adequacy of AT Program implementation. AT Program Reviews shall evaluate all mandatory AT program elements and assess the viability of AT Plans in view of local operational environment constraints and conditions. DoD Standard 31 also states that the DoD Components may use an HHA or JSIVA in lieu of an annual AT Program Review. OPNAV Instruction 3300.53B further states that a record of the annual review will be maintained for a minimum of 3 years and will be included in command turnover files.

During our analysis of the AT Strategic Plan reports submitted by the regions, we observed that regions were not required to respond to the level of compliance with AT Program Reviews at their subordinate installations. The AT Strategic Plan reporting template provided by USFFC to the regions did not contain a question regarding AT Program Reviews, even though it is one of the sub-objectives of the DoD AT Strategic Plan.

We determined that comprehensive AT Program Reviews had been conducted for 14 of 22 installations within our scope following an approved methodology. However, 13 of these installations had their AT Program Reviews conducted by DTRA JSIVA, CNOIVA, or regional assessment teams (HHA). Only one installation AT department conducted a comprehensive AT Program Review of their own installation. The remaining eight installations had not conducted an AT Program Review nor had methodologies been established at the installations. All installations should remain vigilant in the years in which HHA's are not performed to ensure that comprehensive reviews of their AT programs are conducted as required per guidance.

DoD Standard 32 states that heads of DoD Components shall develop AT Program Review Assessment Team guidelines for the conduct of AT Program Reviews. DoD (Standard 32) and USNORTHCOM guidance both state that AT Program reviews shall be modeled upon the DTRA Antiterrorism Vulnerability Assessment Team Guidelines.

To ensure consistency among installation AT Program Reviews, CNO (N3AT) should clarify guidance to mandate the use of an approved methodology for conducting comprehensive AT Program Reviews. Use of the Joint Antiterrorism (JAT) Guide would satisfy the intent of this requirement as its installation AT Program Review template is based on the same standards referenced in the DTRA Vulnerability Assessment Guidelines (DoD Directive 2000.12 and Instruction 2000.16). However, the JAT guide

has yet to be “pushed” to NMCI computers so installations are generally unable to use the program. Given the classified nature of the information utilized through the JAT guide, manual work-arounds (using JAT on stand-alone classified laptops, or utilizing hard-copy JAT-related templates) were not always available, or did not offer the most efficient means to accomplish AT assessments. CNO should ensure full access to the JAT guide for all Navy installation AT personnel.

Antiterrorism Strategic Plan Reporting Tools

The intent of the AT Strategic Plan reporting process is to report compliance and the completion percentage achieved each year for each sub-objective in the AT Strategic Plan. Goals and sub-objectives are noted as “completed” regardless of whether the level of compliance changes in the following year.

We learned that the Navy has not developed or mandated a set of internal controls or checks and balances to ensure that the Navy continues to maintain a previously reported level of compliance. Based on the intent of the DoD/Navy AT Strategic Plan reporting process, and because of the discrepancies noted in the previous section, we concluded that the current USNORTHCOM/USFFC reporting process does not appear to be an effective means to accurately track and validate the progress of Navy installations in meeting and maintaining compliance with DoD and Navy AT standards and associated AT Strategic Plan sub-objectives.

To address this issue the NAVAUDSVC is making the following recommendation (Recommendation 2) to CNO (N46), “Develop controls (in the form of a Web-based tracking system) and implement guidance to ensure that regional commands provide oversight by validating installation-level compliance with DoD/Navy AT standards and associated AT Strategic Plan sub-objectives.”

To ensure ongoing compliance with DoD and Navy AT standards, as well as enhance visibility and oversight, as part of Recommendation 2 CNO (N46) should develop and implement a Web-based, real-time, automated reporting and tracking system. This system should include the capability to attach supporting documentation and/or dates of completion. By providing this capability and control mechanism, greater assurance regarding levels of compliance will be obtained, and more accurate reporting to HHQs such as CNO (N3AT)/(N46), USNORTHCOM, and ultimately OSD will occur. To implement an effective tracking and validation system, CNO (N46) should develop clear guidelines and mandate specific steps that Navy installations and regions must take to satisfactorily input and validate successful completion of annual requirements as mandated/promulgated by DoD/Navy AT Standards and corresponding AT Strategic Plan sub-objectives.

Senior leadership within the Navy – CNO (N3AT), USFFC, and/or the regions – would benefit from the development of a tracking tool designed to measure and report compliance with DoD/Navy AT standards on an annual or recurring basis. Such a tool would provide a steady flow of accurate and timely information, allowing senior leaders to make fully informed decisions regarding the Navy’s AT Program. Once the Navy meets the AT Strategic Plan goals and sub-objectives, this system would help to ensure that the Navy continually maintains the established level of compliance.

Further, the development of an automated, web-based, real-time tracking tool would alleviate the requirement for compiling and sending reports. Such a system would facilitate verification and validation of compliance with DoD/Navy AT Standards and associated AT Strategic Plan sub-objectives if supporting documentation were attached with the entries. This tool should include categories that would require installations to identify and document and support their level of compliance with AT Strategic Plan sub-objectives. To be fully effective, the Navy should identify the standards and conditions necessary to adequately complete a sub-objective. For each sub-objective, CNO (N3AT) should consider including the following categories to help verify installations compliance:

1. Status, progress, or date of completion;
2. Date entered into the system (automatic);
3. “Reported by” field (Point of Contact (POC));
4. “Verified by” field (POC);
5. Supporting documentation attachment-field; and
6. Plan of action for compliance.

Several tracking and compliance tools that have already been established and are currently in use at various Navy commands could be considered by CNO (N3AT) to provide a standardized approach throughout the Navy.

Antiterrorism Readiness Management System (ARMS)

ARMS was developed by a contractor for the Navy and was purchased and is currently used by Commander, Navy Region Southeast (CNRSE). The system was designed to provide a centralized communication portal that manages Antiterrorism/Force Protection readiness data between Navy Echelon II, regional, and installation commands.

CNRSE and officials representing the contractor that developed ARMS noted that it has the “real-time” capability to track and maintain documentation on installation exercises, POCs, and publications and messages; and it contains an events calendar. Further, it was noted that ARMS can be modified to include tracking and verification of compliance with the 35 AT Strategic Plan sub-objectives, to include associated supporting-

documentation or data. Comment boxes (modules) can be included in the system for the installations to respond and provide feedback/comments regarding their status on each section. Since the program is owned by CNRSE, ARMS can be disseminated throughout the Navy without any additional expenditure for the acquisition of the core system and software; however, contractor support, if necessary and requested, would require additional funding. According to CNIC officials, limited ARMS capability (read- or view-only) is currently included within CNIC's Command, Control, Communications, Computers, and Intelligence (C4I)-suite.

Commander, Pacific Fleet (COMPACFLT) Tracking System

COMPACFLT has also internally developed and established a database-tracking mechanism to enhance the tracking and reporting of regional and installation-level compliance with AT Strategic Plan goals and sub-objectives. According to COMPACFLT officials, the program is very adaptable and can easily be changed, such as by adding new objectives or potentially attaching documentation as necessary. It includes a review and verification function for each AT Strategic Plan sub-objective, and is currently capable of developing reports. These reports have progress charts, as well as rollup capabilities to display percentages by installations, regions, or COMPACFLT as a whole. The data is maintained and can be reported for the current or previous fiscal years. The program is considered to be Navy-developed software and would not require additional funding to implement throughout the Navy.

CVAMP

The Core Vulnerability Assessment Management Program (CVAMP) includes an AT Strategic Plan sub-objectives tracking module that allows for color coding – green (acceptable), amber (minimally acceptable), and red (unacceptable). However there is no guidance requiring this information to be filled out by installations and as a result, we found that most installations are not using this function of CVAMP. Further, the CVAMP module is not capable of allowing installation officials to provide substantiation or evidence of compliance with each sub-objective. Without the ability to verify and validate the accuracy of inputs to the system, the usefulness of the module to HHQ would be limited.

DRRS-N

USFFC officials stated that Defense Readiness Reporting System/Navy (DRRS-N) was used to track compliance with AT Strategic Plan sub-objectives. However, we reviewed DRRS-N and determined that its current functional reporting elements do not correspond to any of the 35 AT Strategic Plan sub-objectives.

Currently, USFFC is required to report on only eight Mission Essential Tasks (METs) – only one of which marginally relates to Antiterrorism or Force Protection: “provide

security.” However this MET is very generic and does not provide any visibility of the 5 goals and 35 sub-objectives outlined in the DoD/Navy AT Strategic Plan. According to USFFC officials, DRRS-N will eventually include all the elements of the AT Strategic Plan. If DRRS-N were modified, USFFC and CNO (N3AT) would have to ensure that a mechanism were incorporated to allow installation and regional officials to input documentation, dates, or other information as a means to verify and validate the accuracy of reported levels of compliance with DoD/Navy AT Standards and associated AT Strategic Plan sub-objectives. Without creating a robust system that contains a validation mechanism, DRRS-N would provide little more assurance than the quarterly reporting process currently in place.

CVAMP Implementation

CVAMP and POA&Ms are useful tools that, if fully employed, will allow installations to maintain historic and current records of vulnerabilities requiring installation and higher echelon attention and/or oversight. To fully employ a comprehensive risk management strategy, all vulnerabilities (identified in either integrated vulnerability assessments, higher headquarters assessments, or local vulnerability assessments) must be tracked, validated, and subsequently mitigated or eliminated.

Only after these vulnerabilities and possible mitigation actions are identified and prioritized can management provide the necessary oversight to ensure that these risks are addressed appropriately and effectively. By consistently using management tracking tools such as CVAMP and developing corresponding POA&Ms, Navy commands at all echelons can more effectively track progress toward solutions and ensure that the intended course of action remains accurate, timely, and executable.

Vulnerabilities Analysis

According to DON guidance, vulnerability assessments are to be conducted annually at all Navy installations. During a given 3-year period, the following vulnerability assessments are mandated: a JSIVA or CNOIVA, and two local vulnerability assessments conducted by the installation itself or the installation’s region. DoD, USNORTHCOM and OPNAV guidance clearly state that CVAMP should be populated with vulnerabilities identified during assessments, and that mitigation actions are to be developed and/or identified.

To determine the extent to which CVAMP is populated with assessment-identified vulnerabilities (per DoD, USNORTHCOM, and OPNAV guidance), the audit team performed an analysis of CVAMP entries at 22 CONUS Navy installations covering the most recent 3-year cycle (2005-2007), potentially yielding a total of 66 vulnerability assessments for analysis. We found that required Vulnerability Assessments during this

3-year period had not been conducted at 13 of 66 installations. Vulnerabilities identified within 11 assessments were not verifiable as part of this analysis because installation and region officials were unable to provide copies of the assessments upon request. As a result, we obtained only 42 of 66 VAs for analysis. OPNAV Instruction 3300.53B states that, “A record of the annual review (i.e., date and results) will be maintained for a minimum of 3 years and be included in command turnover files.”

The majority of the installations in our audit scope had consistently entered vulnerabilities into CVAMP over the most recent 3-year period evaluated (2005-2007). However, opportunities for improvement exist. Of the 42 vulnerability assessments obtained for analysis, 6 called for subjective judgment in determining the amount of identified vulnerabilities. As a result, we reviewed the remaining 36 vulnerability assessments and determined that 437 vulnerabilities had been identified over this 3-year period. Of the 437 vulnerabilities identified (and with corresponding VAs available for analysis), only 296 (68 percent) were entered into CVAMP, and 141 were not.

While we identified various underlying causes for vulnerabilities not being entered into CVAMP by installation AT personnel (such as a lack of sufficient manpower), we found that lack of dedicated and reliable SIPRNET access to be the most prevalent cause as 2 of 6 regions and 13 of 22 installations did not have dedicated and/or reliable access to SIPRNET. This greatly hindered those installations’ AT officials from complying with CVAMP requirements.

CNO (N46) should ensure that all CONUS Navy installations have dedicated and reliable SIPRNET access to facilitate use of CVAMP. Further, they should implement controls and oversight to ensure that all Navy installations fully comply with current DoD, USNORTHCOM, and DON guidance concerning CVAMP.

Plans of Action and Milestones (POA&M)

Lack of POA&M Guidance

POA&Ms are an integral part of mitigating and eliminating vulnerabilities; however, there is a lack of clear guidance regarding implementation expectations or requirements. DoD Instruction 2000.16 states in section E3.6.1.2, “Within 90 days of a completed assessment, prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report to the first general officer, flag officer, or civilian equivalent director in the chain of command the results of the assessment.” Similar guidance exists within USNORTHCOM and DON guidance. While criteria states that the installations are required to have a mitigation plan in place for each vulnerability, it does not state that mitigation plans must be entered into CVAMP, or what should be contained within the mitigation plans. Constructing consolidated POA&Ms for both higher headquarters assessments and annual self-assessments is important for developing

and managing mitigation efforts and ensuring that necessary AT unfunded requirements are generated for consideration in future budget submissions.

When determining necessary actions to mitigate an identified vulnerability, the type of vulnerability must be considered (programmatic or procedural). Procedural vulnerabilities can be mitigated without funding by implementing or changing an installation's operating procedures. For example, a common procedural vulnerability identified within CVAMP, "access control procedures at gates are inconsistent, poorly defined, outdated," could be mitigated with a change in security plans, but will not require funding to complete. Conversely, programmatic vulnerabilities can be eliminated only with funding. This includes common Access Control Point (ACP) vulnerabilities identified within CVAMP such as, "Active vehicle gates are subject to high speed and have no positive stopping capability." However, funding may not be readily available, so temporary mitigation measures should be in place to lower the risk to the ACP, such as increasing patrols, and modifying barrier plans. When funding is not readily available, the ATO should develop and implement procedural measures to mitigate the programmatic vulnerabilities until funding becomes available.

If CVAMP and the tools therein (i.e., Corrective Action section for POA&Ms) are consistently implemented and updated, commands can more effectively track an installation's progress toward the mitigation and elimination of vulnerabilities.

POA&M Best Business Practices

As explained in the prior section, while there is criteria that states that installations are required to have a POA&M in place for each vulnerability, there is no guidance that defines what represents (or should be included within) an effective POA&M. This creates the potential for inconsistencies in POA&M content. Our analysis indicated a significant degree of variation in the type of information included in POA&Ms throughout the installations within our scope. Using examples of POA&M best business practices would alleviate many of the discrepancies found across the installations we visited. Based on best business practices and the format provided in Office of Management and Budget (OMB) memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," dated 17 October 2001, we determined that an effective and executable POA&M should include the following elements:

- A description of the vulnerability and the plan of mitigation;
- A point of contact who will be responsible for resolving the weakness;
- A scheduled completion date for resolving the weakness;
- Key milestones (as applicable) with completion dates; and
- Notation of the corrective action when a milestone is reached.

These five items can be entered into CVAMP via the corrective action section, which contains areas for mitigation measures, corrective actions, POC, start and end dates, percentage completed, and any additional comments needed. We recommend that CNO create criteria based on these best business practices to allow for a more consistent and uniform approach in developing POA&Ms across the Navy, thereby facilitating proper and timely mitigation of vulnerabilities.

POA&M Analysis

An analysis was performed to determine if POA&Ms have been developed and entered into CVAMP for their associated vulnerabilities at 21 of the 22 the installations within our audit scope.⁶ The audit team determined the status and nature of mitigation measures developed and entered into CVAMP by the 21 installations. The scope of the analysis consisted of POA&Ms for associated vulnerabilities identified (over the 3-year period 2005-2007) within JSIVAs, CNOIVAs, regional and Higher Headquarters Vulnerability Assessments, and Local Vulnerability Assessments (LVAs) that were entered into CVAMP. The 437 vulnerabilities identified earlier which had been analyzed for CVAMP-entry-compliance only constitute the universe of vulnerabilities identified within hard copy Integrated Vulnerability Assessments (IVAs) received from installations within our audit scope. On the other hand, POA&M analysis consists of 448 vulnerabilities that we observed within CVAMP over the 2005-2007 period; these vulnerabilities located within CVAMP were analyzed regardless of verification from hard copy IVAs.

Our review of CVAMP vulnerabilities determined that 35 percent of all entries (155 of 448) did not have a POA&M. Our analysis also identified the following weaknesses:

- 37 (approximately 8 percent) did not contain a Mitigation Action Plan (MAP) and dates, but included a POC;
- 57 (approximately 13 percent) contained a POA&M that had been misplaced in the “Vulnerability Summary” area of CVAMP (limits visibility of POA&M);
- 29 (approximately 6 percent) contained completion dates and/or a POC, but did not include a MAP; and
- 9 (approximately 2 percent) miscellaneous POA&M issues.

Although most entries did not contain some elements of an effective POA&M, we learned that:

⁶ One region and installation are excluded from our data because of their inability to enter assessments into CVAMP because they lack SIPRNET capability.

- 30 of 448 vulnerabilities (approximately 7 percent) contained a sufficient MAP, POC, and start and end and/or interim dates (contained all elements of an effective POA&M); and
- 101 (approximately 22 percent) contained a MAP and POC, but no dates (contained most elements of an effective POA&M).

Finally, we found that 30 (7 percent) were listed as “Risk Accepted by Commanding Officer (CO)” and therefore did not contain a MAP.

Adequate POA&Ms

Robust POA&Ms located within the correct area of CVAMP ensures that actions taken to mitigate or eliminate identified vulnerabilities are visible to senior leadership. Of vulnerabilities with information entered in the correct area of CVAMP, only 30 contain a MAP, start and end and/or interim dates, and a POC as identified in the best business practices section above. These are considered to be complete POA&Ms, per best business practices. Additionally, 101 POA&Ms contain a MAP and a POC, but no interim dates. Listing the action being taken, the date the project will be started and approximately ended, as well as any updates to the project and a point of contact, allows upper echelon officials to maintain visibility of the actions being taken to eliminate the vulnerability. With start and end dates, installation officials will be more accountable for mitigating vulnerabilities in a timely fashion.

Inadequate POA&Ms

Of the 448 identified vulnerabilities, 155 did not have any POA&M information entered into CVAMP, while 37 included only a POC, and 29 included only start and end dates. As a result, 49 percent of vulnerabilities within our sample had no mitigation action plan. The audit team identified this as a systemic problem, affecting all five regions included within this analysis.⁷ DoDI 2000.16 states that installations are required to have a mitigation plan in place for each vulnerability, but it does not state that mitigation plans must be entered into CVAMP. The high rate of vulnerabilities without mitigation plans may be attributed to a lack of criteria. The lack of POA&Ms entered into CVAMP does not necessarily indicate that there are no actions in place to mitigate the vulnerabilities. Seven installations within our scope have hard copy POA&Ms. However, it is important to enter POA&Ms into CVAMP to allow for sufficient visibility and to aid in competition for limited funding. In our opinion, installations should consider maintaining written POA&Ms as a best business practice, in addition to having the POA&Ms recorded in CVAMP in light of the frequent SIPRNET access issues experienced.

⁷ Commander, Navy Region Midwest (CNRMW) was not included within this analysis, as no vulnerabilities had been entered into CVAMP for CNRMW due to lack of reliable SIPRNET.

Risk Acceptance

Within CVAMP, risk can be accepted for some vulnerabilities. Not all vulnerabilities can be mitigated – a lack of perimeter standoff between buildings and the outlying installation perimeter are among the most common examples because funding for blast walls, or moving the building, is generally prohibitive. In these select cases in which a vulnerability cannot be realistically mitigated, installation commanders are allowed to “accept risk” instead of entering a POA&M. To reduce this burden on installation COs, CNO N3/N5 issued a memorandum in June 2008, noting that forthcoming policy changes will identify and quantify the degree of risk that OPNAV will assume in the AT mission area.

SIPRNET

CVAMP resides solely on the SIPRNET, the DoD’s Secure Internet system for information classified up to the Secret level. DoD O-2000.12P, “DoD Antiterrorism Strategic Plan,” states that, “By the end of FY 2010, JSIVA and HHA trends shall reflect that 90 percent of designated ATOs, including those assigned or attached to in-transit units, have dedicated access to SIPRNET.” Although NMCI is currently rolling out the new SIPRNET system across CONUS installations, connectivity and access to SIPRNET-ready computers is inconsistent throughout the 22 installations and 2 of the 6 regions we visited. In total, 8 installation ATOs did not have dedicated access to SIPRNET, and only a few had received and been switched over to NMCI SIPRNET.

We learned that selected regions and installations are forced to identify and develop “workarounds” for accessing SIPRNET. One region we visited has little to no connectivity with SIPRNET, so the responsibility to maintain, manage, and update CVAMP was assigned to one of their subordinate installation ATOs. This does not allow the regional ATO to consistently review and update CVAMP every month, as required by USNORTHCOM guidance. AT personnel at one of six regions, as well as 8 (of 22) installations found it necessary to access SIPRNET from another location or site, either on post or at another installation within the region. Without dedicated access to SIPRNET, selected regional and/or installation AT personnel may be unable to perform all required CVAMP-related responsibilities and effectively and efficiently respond to taskers from HHQs in a timely fashion, to include:

- Entering identified vulnerabilities into CVAMP;
- Reviewing and forwarding installation CVAMP entries and Combating Terrorism Readiness Initiative Fund (CbTRIF) funding requests; and
- Receiving and responding to classified messages from HHQ (CNIC, CNO, and USFFC) such as changes in FPCON levels or participating in exercises such as DoD-wide Solid Curtain.

While many installations and regions are actively trying to find ways to mitigate this problem, the necessary work-arounds that have been identified and developed to alleviate connectivity problems can be time-consuming and inefficient. In anticipation of this difficulty, USNORTHCOM guidance (05-01B) assigns responsibility to higher commands and states that, “If the facility does not have SIPRNET access, or otherwise does not have the capability to enter data into CVAMP, then a written report will be mailed, by traceable means (i.e., registered mail) to the next higher office in the chain of command capable of inputting data into CVAMP. In this case, it may be difficult to meet the time requirements identified above; however, required data should be entered into CVAMP as expeditiously as possible.” CNO should ensure that upper echelons (regional or USFFC officials) are following guidance and continuing to assist installations and regions with CVAMP implementation to mitigate and eliminate vulnerabilities until dedicated SIPRNET access is secured at both the installation and regional level.

CNO (N3AT) should ensure that all Navy CONUS installations receive dedicated access to SIPRNET, to allow for efficient and timely AT execution.

Conclusion

We determined that the Navy lacked an adequate tracking and control system that validates reported AT Strategic Plan sub-objective compliance levels. As a result, we identified installation-level AT Strategic Plan compliance and reporting discrepancies.

We also determined that Navy installations audited had not consistently entered all identified vulnerabilities into CVAMP. We identified a lack of dedicated and reliable SIPRNET access to be the most prevalent cause for installations not entering identified vulnerabilities into CVAMP.

Finally, we determined that the Navy has not established guidance that mandates that POA&Ms be entered into CVAMP, nor has the Navy developed a standardized methodology outlining required elements of a POA&M. As a result, Navy installations had not consistently created POA&Ms and entered them into CVAMP.

Recommendations

The Office of the Chief of Naval Operations (CNO) (N3AT) responded to Recommendation 1, and CNO (N46) responded to Recommendations 2-9. Summaries of the management responses, with our comments, are below. The full text of the management responses is in the Appendices.

We recommend that Chief of Naval Operations (CNO) Antiterrorism (N3AT):

Recommendation 1: Develop procedures establishing CNO (N3AT)'s involvement in the Antiterrorism (AT) Strategic Plan reporting process to ensure sufficient visibility to aid in making both AT-related procedural (requirements/manpower) and programmatic (funding) decisions.

CNO (N3AT) response to Recommendation 1: Concur. In accordance with DoDI 2000.16, Navy Component Commanders will conduct annual AT program reviews. A summary of the assessments, program trends, and program initiatives will be forwarded to OPNAV (N3AT) no later than 1 November. The command will have visibility of the web-based compliance tool established by CNO N46 (Recommendation 2) and review annual results to ensure compliance with AT standards and Strategic Plan sub-objectives. The target completion date is 31 December 2008.

Naval Audit Service comment on the response to Recommendation 1: Actions planned by CNO N3AT meet the intent of the recommendation.

We recommend that CNO (N46):

Recommendation 2: Develop controls (in the form of a Web-based tracking system) and implement guidance to ensure that regional commands provide oversight by validating installation-level compliance with DoD/Navy AT standards and associated AT Strategic Plan sub-objectives.

CNO (N46) response to Recommendation 2: Concur. CNO N46 will ensure compliance with AT standards and Strategic Plan sub-objectives through establishment of a web-based tool for regional oversight. Discussion of existing Government-owned systems and possible alternatives will occur at the January 2009 C4I Policy Standards Board. The target completion date is 31 March 2009.

Naval Audit Service comment on response to Recommendation 2: In subsequent communication, N46 noted that usage of the Web-based system would (at the regional level) be mandated within OPNAV 3300.53 series guidance. Actions planned by N46 meet the intent of the recommendation.

Recommendation 3: Establish the required frequency of installation Antiterrorism Working Group (ATWG) meetings; clarify and document required meeting frequency in guidance to ensure the requirement is consistently followed by installations.

CNO (N46) response to Recommendation 3: Concur. N46 will coordinate with OPNAV N3AT to ensure that ATWG requirements are included and clearly articulated in OPNAV AT policy (3300.53 series), which is currently under revision; the instruction will mirror the ATWG frequency requirements established by the DoDI 2000.16 (Paragraph E3.10) requiring the ATWG meet at least semi-annually. The target completion date is 31 October 2008.

Naval Audit Service comment on response to Recommendation 3: Actions planned by N46 meet the intent of the recommendation.

Recommendation 4: Develop an annual AT program review tool, and clarify guidance mandating its use at both the regional and installation level.

CNO (N46) response to Recommendation 4: Concur. N46 will establish the review tool and guidance. By 15 January 2009, N46 will determine if the existing Joint Antiterrorism (JAT) guide can be augmented to satisfy this requirement. By 30 April 2009, N46 will also work with CNIC N3AT/N5 to develop alternatives in lieu of JAT including entries in the existing DRRS-N reporting tool. The target completion date is 31 August 2009.

Naval Audit Service comment on response to Recommendation 4: Actions planned by N46 meet the intent of the recommendation. Because the target completion date is more than 6 months in the future, CNO (N46) should provide a status report by the 15 January 2009 date to determine if the JAT guide can be augmented, and by the 30 April 2009 date to develop alternatives in lieu of JAT.

Recommendation 5: Clarify guidance regarding usage of the JAT guide to develop installation AT Plans and conduct required annual AT assessments and AT Plan reviews. Further, develop an implementation plan to ensure that all Continental United States (CONUS) Navy Installation AT personnel have access to the JAT guide.

CNO (N46) response to Recommendation 5: Concur. In coordination with N46, CNIC will issue an updated CNIC 5530-series Security Program Manual that will include specific implementation guidance for the utilization of the JAT guide. CNIC has also begun providing JAT training and assistance to regional staffs that will reach out to Navy installations. CNIC will also explore the possibility of including the JAT Guide in the C4I Suite. The target completion date is 31 December 2008.

Naval Audit Service comment on response to Recommendation 5: In subsequent communication, N46 officials affirmed their intent to

implement a plan to ensure that CONUS Navy installation AT personnel have access to the JAT guide. Actions planned by N46 meet the intent of the recommendation.

Recommendation 6: Develop controls and provide oversight to ensure that current guidance regarding Core Vulnerability Assessment Management Program (CVAMP) responsibilities at both the regional and installation level are adhered to, ensuring that identified vulnerabilities are entered within CVAMP, and that installation-level AT-related assessments are properly performed, documented, and retained in official files.

CNO (N46) Response to Recommendation 6: Concur. CNIC Instruction 3300.1, Risk Analyzed Mitigation Process (RAMP) (signed 29 July 2008), directed Regions and Installations to adhere to the process of entering vulnerabilities into CVAMP. Oversight is provided via the RAMP program, whereby Naval Facilities Engineering Service Center (NFESC) engineers physically attend Joint Staff and/or CNO IVA out-briefs and assist Navy installations with receipt and disposition of that information and provides training to the installation CVAMP operator as necessary. It is anticipated that all 78 CNIC installations will receive this service over a 3-year period. By the interim completion date of 31 March 2009, the details and measures of RAMP will become an OPNAV Instruction, most likely included into the existing 3300.53 series, to ensure oversight at the Echelon I level as required and to establish an enduring process beyond the currently funded 3-year RAMP initiative. The target completion date is 30 September 2010, with an interim completion date of 31 March 2009.

Naval Audit Service comment on response to Recommendation 6: The actions planned by N46, when combined with actions planned in response to Recommendation 2, meet the intent of the recommendation. CNO N46 should provide a status report by the 31 March 2009 interim target date.

Recommendation 7: Develop an implementation plan to ensure that all CONUS Navy installations have dedicated and reliable Secure Internet Protocol Router Network (SIPRNET) access to facilitate use of CVAMP.

CNO (N46) Response to Recommendation 7: Concur. N46, in coordination with OPNAV N6 (Communication Networks, resourcing division), will develop a strategy for SIPRNET implementation with an established timeline for logical deployment to all SIPR/OneNet systems during the period of 2-21 October 2008. The target completion date is 31 August 2009.

Naval Audit Service comment on response to Recommendation 7: The actions planned by N46 meet the intent of the recommendation. Because the target completion date is more than 6 months in the future, CNO (N46) should provide a status report by 31 March 2009 on the progress in implementing a SIPRNET strategy.

Recommendation 8: Develop controls, implement guidance, and provide oversight to ensure that AT personnel develop (and enter into CVAMP) effective Plans of Action and Milestones (POA&Ms) for tracking, reporting, and mitigating or eliminating vulnerabilities.

CNO (N46) Response to Recommendation 8: Concur. The RAMP process, referenced in Recommendation 6, is designed to assist installations with determining mitigation strategies. By the interim completion date of 31 March 2009, RAMP will also provide a database of past mitigation strategies to vulnerabilities as a reference to installation Security officers. Target date for completion of all installation assessments is 30 September 2010, the same as Recommendation 6. The target completion date is 30 September 2010 with an interim completion date of 31 March 2009.

Naval Audit Service comment on response to Recommendation 8: Actions planned by N46, when combined with actions planned in response to Recommendation 9, meet the intent of the recommendation. CNO (N46) should provide a status report by the 31 March 2009 interim target date.

Recommendation 9: Develop guidance defining the minimum required elements to be included within POA&Ms.

CNO (N46) response to Recommendation 9: Concur. N46 plans to work with NFESC on outlining minimum required information for installation POA&Ms. CNIC will make changes to CNIC Instruction 3300.1 (RAMP) and forward revision to OPNAV N46 for inclusion into policy that will specify POA&M criteria. The target completion date is 31 March 2009.

Naval Audit Service comment on responses to Recommendation 9: The actions taken and/or planned by CNO (N46) meet the intent of the recommendations. Additionally, per N46's response to Recommendation 6, RAMP guidance will be included within OPNAV guidance to ensure an "enduring process" beyond the current RAMP cycle.

Section B:

Status of Recommendations

RECOMMENDATIONS						
Finding ⁸	Rec. No.	Page No.	Subject	Status ⁹	Action Command	Target or Actual Completion Date
1	1	21	Develop procedures establishing CNO (N3AT)'s involvement in the AT Strategic Plan reporting process to ensure sufficient visibility to aid in making both AT-related procedural (requirements/manpower) and programmatic (funding) decisions.	O	CNO (N3AT)	12/31/2008
1	2	21	Develop controls (in the form of a web-based tracking system) and implement guidance to ensure that regional commands provide oversight by validating installation-level compliance with DoD/Navy AT standards and associated AT Strategic Plan sub-objectives.	O	CNO (N46)	3/31/2009
1	3	21	Establish the required frequency of installation ATWG meetings; clarify and document in guidance to ensure the requirement is consistently followed by installations.	O	CNO (N46)	10/31/2008
1	4	22	Develop an annual AT program review tool, and clarify guidance mandating its use at both the regional and installation level.	O	CNO (N46)	1/15/2009
1	5	22	Clarify guidance regarding usage of the Joint Antiterrorism (JAT) guide to develop installation AT Plans and conduct required annual AT assessments and AT Plan reviews. Further, develop an implementation plan to ensure that all CONUS Navy Installation AT personnel have access to the JAT guide.	O	CNO (N46)	12/31/2008
1	6	23	Develop controls and provide oversight to ensure that current guidance regarding CVAMP responsibilities at both the regional and installation level are adhered to, ensuring that identified vulnerabilities are entered within CVAMP, and that installation-level AT-related assessments are properly performed, documented, and retained in official files.	O	CNO (N46)	3/31/2009
1	7	23	Develop an implementation plan to ensure that all CONUS Navy installations have dedicated and reliable SIPRNET access to facilitate use of CVAMP.	O	CNO (N46)	8/31/2009
1	8	24	Develop controls, implement guidance, and provide oversight to ensure that AT personnel develop (and enter into CVAMP) effective POA&Ms for tracking, reporting, and mitigating or eliminating vulnerabilities.	O	CNO (N46)	3/31/2009
1	9	24	Develop guidance defining the minimum required elements to be included within POA&Ms.	O	CNO (N46)	3/31/2009

⁸ / + = Indicates repeat finding

⁹ / 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

Background

Antiterrorism (AT) is defined as defensive measures taken to reduce vulnerability to terrorist attacks. Installation commanders are required to develop prescriptive AT standards based on the installation location, potential threat, and the operating environment. They shall also clearly establish AT responsibility for all units and individuals under their command.

The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against Department of Defense (DoD) personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment, as well as the preparation to defend against and plan for response to the consequences of terrorist incidents. For an installation's AT program to accomplish this goal, it is essential to ensure that resources are available to execute the AT plan that accomplishes the following: deterring terrorist incidents; employing countermeasures against terrorists; mitigating the effects of terrorist attacks; and responding to and recovering from terrorist incidents should they occur.

The AT Strategic Plan was developed to ensure that the most critical elements of an AT Program are being achieved, therefore satisfying the intent of reducing vulnerabilities to terrorist attacks. The plan's 5 goals and 35 supporting performance objectives are designed to provide a framework for DoD components to follow when developing a robust AT Program.

The Core Vulnerability Assessment Management Program (CVAMP) is a tool used to track the status of assessment identified installation vulnerabilities. If implemented fully, CVAMP allows all command levels to maintain visibility of vulnerabilities and track in-progress mitigation actions. This program should be used to submit funding requests for the mitigation of vulnerabilities through the Combating Terrorism Readiness Initiatives Fund (CbTRIF).

Scope and Methodology

Scope

Considering cycle-time requirements and limitations, we determined that an audit scope consisting of all Navy regions and installations would not allow for timely completion and issuance of the audit report. We focused our audit work only on the six CONUS regions and a judgmental sample of subordinate installations, generating an audit scope based on installation manning levels as a determining factor for selection. As a result, our review encompassed all 6 CONUS Navy regions and 22 judgmentally-selected installations with 4,000 personnel (or more). (These and other activities that we visited and/or contacted are listed in Exhibit C).

We analyzed how effectively selected installations within the six Navy Regions in the U.S. Northern Command's (USNORTHCOM's) area of responsibility (AOR) have complied with the AT Strategic Plan objectives while developing and executing a robust AT Program. We also analyzed the accuracy and adequacy of information entered by installation officials into the CVAMP system. Our work was conducted from 30 October 2007 through 28 August 2008.

To allow for the widest dissemination of this report and for security reasons, we do not identify by name specific installations where potential vulnerabilities or general AT weaknesses have been identified. These AT-related observations have also been shared, through the issuance of point papers, with appropriate regional and installation officials. This information is marked For Official Use Only and is available upon request on a need-to-know basis.

Methodology

We focused on 15 of the 35 sub-objectives of the Department of Defense (DoD) O-2000.12P which in our opinion, were most pertinent to the execution of a robust Antiterrorism (AT) program for an installation. We also reviewed all applicable DoD and Department of the Navy (DON) directives, instructions and guidance. We provided point papers to each of the six regions audited at the conclusion of each of the regional site visits detailing noteworthy accomplishments and areas of concern at both the regional and installation level.

We determined how each region and installation visited reported their progress in meeting standards set in Office of the Chief of Naval Operations (OPNAV) Instruction 3300.56 in the quarterly AT Strategic Plan submission. We met with higher headquarters AT officials to determine their level of oversight/visibility of the quarterly reports, and what was done with this information. We obtained and analyzed installations'

documentation to verify that the quarterly reports sent to higher headquarters by each region are reported accurately.

We determined whether installations prepared and performed threat, criticality, and local vulnerability assessments containing all required elements established in DoD and DON guidance. We determined whether formal risk assessments were conducted at each installation in accordance with DoD Instruction 2000.16.

We determined whether all 22 installations we visited had an updated, properly classified, and signed AT Plan. We also determined the extent of regional oversight toward installation AT Plans.

We held meetings with higher echelons to discuss the level of oversight provided to the installations, installation Antiterrorism Official (ATO) requirements and responsibilities, and AT reporting requirements to higher echelons. We determined whether roles and responsibilities of installations had been clearly established.

We determined whether installations had Joint Staff Integrated Vulnerability Assessments (JSIVA) or Chief of Naval Operations Integrated Vulnerability Assessments (CNOIVAs) conducted at their installations every 3 years in accordance with DoD standards. We also determined whether installations were performing local vulnerability assessments in years that higher headquarters assessments had not been conducted. We determined whether Plans of Actions and Milestones (POA&Ms) or any other mitigation plan had been established for vulnerabilities identified during vulnerability assessments. We reviewed installation CVAMP entries to determine if CVAMP had been fully implemented. We determined the adequacy of Secure Internet Protocol Router Network (SIPRNET) at both the regional and installation level.

We determined whether regional and installation AT officials had established all required working groups in accordance with DoD and DON guidance.

We reviewed the assessments/program reviews provided by Chief of Naval Operations (CNO) (N3AT); United States Fleet Forces Command (USFFC) (N3AT); and Commander, Navy Installation Command (CNIC) (N3AT) to determine the scope of the review, types of issues identified by the reviews or assessments, when the reviews or assessments took place, and recommendations relevant to our audit.

We determined whether each region conducted AT Program reviews of their installations, and whether the installations conducted an annual review of their AT Programs. We also determined the methodology used for conducting these reviews.

We conducted this 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.

Activities Visited and/or Contacted

- Office of the Secretary of Defense, Special Operations/Low Intensity Conflict*
- United States Northern Command
- Chief of Naval Operations (N3AT)*
- United States Fleet Forces Command*
- Commander, Navy Installations Command*
- Naval Criminal Investigative Service*

6 Regions and 22 Installations Visited/Contacted

- Commander, Naval District Washington*
- Commander, Navy Region Northwest*
- Commander, Navy Region Midwest*
- Commander, Navy Region Southwest*
- Commander, Navy Region Mid-Atlantic*
- Commander, Navy Region Southeast*
- Naval Support Activity Washington*
- Naval Air Station (NAS) Patuxent River*
- Naval Station Everett*
- Naval Base Kitsap*
- NAS Whidbey Island*
- Naval Station Great Lakes*
- Naval Base Coronado*
- NAS Lemoore
- Naval Base Point Loma*
- Naval Base San Diego*
- Naval Amphibious Base Little Creek*
- Naval Station Newport
- Naval Submarine Base New London
- Naval Station Norfolk*
- Norfolk Naval Shipyard*
- NAS Oceana*
- Naval Weapons Station Charleston
- Naval Construction Battalion Center Gulfport
- NAS Jacksonville*
- Naval Submarine Base Kings Bay*
- Naval Station Mayport*
- NAS Pensacola*

* Activity Visited

Pertinent Guidance

Department of Defense (DoD) Instruction 2000.16 “DoD Antiterrorism Standards,” dated 2 October 2006, requires that the risk management process and procedures are to be reviewed at least annually. The risk assessment process should be modeled after the principles outlined in DoD O-2000.12-H and should be applied in all aspects of AT program implementation and planning, including operational plans and decisions, development of risk mitigation measures, and the prioritization and allocation of resources. Threat, asset criticality, and vulnerability should be considered while conducting risk assessments and are the essential components of AT Risk Management. This instruction also mandates installations to conduct a vulnerability assessment at least annually. The assessment should provide a vulnerability-based analysis of mission-essential assets, resources, and personnel critical to mission success who may be susceptible to terrorist attack.

DoD Instruction 2000.16 also states that Threat Working Groups (TWGs) should meet at least quarterly to develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries. It also states that Antiterrorism Working Groups (ATWGs) and Antiterrorism Executive Committees (ATECs) should be held semi-annually.

DoD Instruction 2000.16 states the heads of DoD components shall, “Consider maintaining full-time AT staffs, including individuals with CBRNE expertise, at the Component Command, installation, separate facility, and other subordinate headquarters levels as appropriate.”

DoD Instruction 2000.16 “DoD Antiterrorism Standards” states that heads of DoD components shall, “Ensure that the DoD vulnerability database (the Core Vulnerability Assessment Management Program (CVAMP)) is populated with all assessment results.”

DoD Instruction 2000.16 “DoD Antiterrorism Standards” states that heads of DoD components shall, “prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report ... the results of the assessment.”

U.S. Northern Command (USNORTHCOM) Antiterrorism Operations Order (OPORD) 05-01B, dated 15 July 2006, states that per DoD Instruction 2000.16, commanders will conduct an annual review of their respective AT Program, as well as that of their immediate subordinates. The OPORD further requires a “documented compliance review of the AT Programs and plans of their immediate subordinates in the chain of

command at least annually.” The guidance also states that the installation commander will designate in writing a commissioned officer, noncommissioned officer, or civilian staff officer as the ATO for each installation.

USNORTHCOM OPOD 05-01B states that “Services/designated AT representatives for the Services will ensure vulnerability data has been registered into the CVAMP by the installation ATO.”

Chief of Naval Operations (OPNAV) Instruction 3300.53B, “Navy AT Program,” dated 28 November 2007, states that CNO (N3AT) is responsible for managing the Navy’s AT Strategic Plan.

OPNAV Instruction 3300.53B states that “A record of the annual review (i.e., date and results) will be maintained for a minimum of 3 years and be included in command turnover files.”

Secretary of the Navy (SECNAV) Instruction 3300.2B “Department of the Navy (DON) Antiterrorism (AT) Program,” dated 28 December 2005, states, “Ensure all AT vulnerability assessment data, being either a self-assessment, HHQ assessment, JSIVA, and/or actions planned/taken to mitigate them, are entered into CVAMP.”

SECNAV Instruction 3300.2B “Department of the Navy (DON) Antiterrorism (AT) Program” states, “Ensure all AT vulnerability assessment data, being either a self-assessment, HHQ assessment, JSIVA, and/or actions planned/taken to mitigate them, are entered into CVAMP.”

OPNAV Instruction 5530.14D, dated 30 January 2007, indicates that ATWGs should meet at least quarterly.

Exhibit E:

List of Acronyms

AOR	Area of Responsibility
ARMS	Antiterrorism Readiness Management System
ASD/HD	Assistant Secretary of Defense/Homeland Defense
AT	Antiterrorism
ATEC	Antiterrorism Executive Committee
ATO	Antiterrorism Officer
ATWG	Antiterrorism Working Group
C4I	Command, Control, Communications, Computers, and Intelligence
CA	Criticality Assessment
CbTRIF	Combating Terrorism Readiness Initiative Fund
CNIC	Commander, Navy Installations Command
CNO (N3AT)	Chief of Naval Operations, Antiterrorism
CNO (N46)	Chief of Naval Operations, Ashore Readiness Division
CNOIVA	Chief of Naval Operations Integrated Vulnerability Assessment
CNRMA	Commander, Navy Region Mid-Atlantic
CNRMW	Commander, Navy Region Midwest
CNRNW	Commander, Navy Region Northwest
CNRNDW	Commander, Naval District Washington
CNRSE	Commander, Navy Region Southeast
CNRSW	Commander, Navy Region Southwest
COCOM	Combatant Command
COMPACFLT	Commander, U.S. Pacific Fleet
CONUS	Continental United States
CVAMP	Core Vulnerability Assessment Management Program
DoD	Department of Defense
DoDD	Department of Defense Directives
DoDI	Department of Defense Instruction
DON	Department of the Navy
DRRS-N	Defense Readiness Reporting System Navy
DTRA	Defense Threat Reduction Agency
EM	Emergency Management
FPCONS	Force Protection Conditions
GAO	Government Accountability Office
GWOT	Global War on Terrorism
POA&M	Plans of Action and Milestones
HHA	Higher Headquarters Assessment
HHQ	Higher Headquarters
JAT	Joint Antiterrorism
JSIVA	Joint Staff Integrated Vulnerability Assessment
MAPs	Mitigation Action Plans
METs	Mission Essential Tasks
NCIS	Naval Criminal Investigative Service
NMCI	Navy/Marine Corps Intranet
OASD & SO/LIC	Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict

OMB	Office of Management and Budget
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
RA	Risk Assessment
SECNAV	Secretary of the Navy
SIPRNET	Secure Internet Protocol Router Network
TA	Threat Assessment
TWG	Threat Working Group
USFFC	U. S. Fleet Forces Command
USNORTHCOM	U.S. Northern Command
VA	Vulnerability Assessment
WMD/CBRNE	Weapon of Mass Destruction/Chemical, Biological, Radiological, Nuclear, or High Yield Explosive

Appendix 1:

Management Response from Office of the Chief of Naval Operations (N3AT)



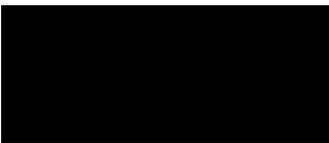
DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO
5530
Ser N3IPS/8U154630
29 Sep 08

From: Director, Information, Plans and Security Division
(N3IPS)
To: Assistant Auditor General, Installation and Environment
Subj: NAVAL AUDIT SERVICE DRAFT REPORT N2008-NIA000-0051.000,
NAVY ANTITERRORISM PROGRAM EXECUTION
Ref: (a) NAVAUDSVC memo 7510/N2008-NIA000-0051.000 dated 28
August 2008
Encl: (1) N3AT response to NAVAUDSVC draft report number N2008-
NIA000-0051.000 of 28 August 2008

1. In response to reference (a), enclosure (1) provides the Director, Information, Plans and Security response to Finding 1 (Navy Antiterrorism Strategic Plan), Recommendation 1 in the subject audit report.
2. Neither our response to the audit recommendations or the report contain information we deem "For Official Use Only."
3. The N3IPS point of contact for this audit is [REDACTED] or [REDACTED]

FOUO (b)(6)



Director, Information, Plans and Security response to Naval
Audit Service Draft Report N2008-NIA000-0051.000

Finding 1: Navy Antiterrorism Strategic Plan

Recommendation 1. Develop procedures establishing CNO(N3AT)'s involvement in the AT Strategic Plan reporting process to ensure sufficient visibility to aid in making both AT-related procedural (requirements/manpower) and programmatic (funding) decisions.

Target completion date: December 31, 2008

Response. Concur. Chief of Naval Operations released a NAVADMIN in June 2008 announcing the realignment of strategic and operational antiterrorism policy and resourcing responsibilities that will ensure the most effective and efficient execution of the Navy's antiterrorism mission. This policy realignment will create an environment that validates requirements and provides commanders and commanding officers with the necessary resources to protect navy assets and personnel while managing risk. The realignment incorporates checks and balances between policy and resourcing, with echelon I oversight, that will result in a viable and executable antiterrorism program. These changes will be codified in OPNAV instructions 3300.53 and 5530.14 series. Specifically, the following roles and responsibilities were assigned:

- OPNAV N3/N5 is responsible for strategic oversight of the Navy's antiterrorism policy, both afloat and ashore. In concert with USFF and NCIS, N3/N5 will set and shape the overall security environment. Additionally, N3/N5 will be responsible for the assessment of afloat and ashore antiterrorism programs to ensure effective compliance with higher level guidance. N3/N5 will also conduct periodic detailed reviews of risk assessments and ensure risk assumed in the antiterrorism mission is consistent with Navy policy. N3/N5 will assess risk in the sponsor program proposals relative to achieving outcomes consistent with antiterrorism policy.

- Fleets will determine antiterrorism requirements and execute the antiterrorism program within their AOR. CNIC will use fleet antiterrorism requirements to develop capability plans and provide input to OPNAV N4 as the ashore resource sponsor. CNIC will conduct periodic ashore AT risk assessments.

Enclosure (1)

- CNO Annual Antiterrorism Assessment - NCIS MTAC will draft an annual strategic world-wide Terrorism threat assessment for the US Navy. This assessment will address adversary capabilities and current threats to Navy assets and personnel. Assessment will be published NLT 1 June.

- CNO Antiterrorism Strategic Guidance - CNO N3/N5 will draft annual guidance for Navy Commander's to utilize in resourcing and addressing the terrorism threat. Specifically, CNO AT Strategic Guidance will comment on current threat assessment, direct appropriate threat posture, list CNO's top 5 AT issues, and prioritize AT efforts. AT Strategic Guidance will be published NLT 1 September.

- CNO Antiterrorism Execution Program Review - IAW DoDI 2000.16, Navy Component Commanders will conduct annual AT program reviews. A summary of the assessments, program trends and program initiatives will be forwarded to OPNAV N3AT NLT 01 November.

- CNO Annual Antiterrorism Sponsor Program Proposals (Afloat & Ashore) Assessment - OPNAV N81 in coordination with PMS-480, USFF N3AT, OPNAV N3AT, and resource sponsors will, as part of its annual Integrated Program Assessment (IPA) and Integrated Capability Plans (ICP), assess the Navy's AT program to determine if CNO's Strategic Guidance and priorities are being met. It will provide recommendations, assess risks, and prioritize change proposals. This assessment will be provided to the CNO each year NLT 01 April IAW applicable N8 POM/PR guidance.

- CNO N3AT will have visibility of the web based compliance tool established by CNO N46P (Recommendation 2) and review annual results to ensure compliance with AT standards and Strategic Plan sub-objectives.

Appendix 2:

Management Response from Office of the Chief of Naval Operations (N46)



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
1100 NAVY BUILDING
WASHINGTON, D.C. 20370-3000

IN REPLY REFER TO
7511
Ser N46/80158483
OCT 06 2008

From: Director, Ashore Readiness Division (N46)
To: Assistant Auditor General, Installation and Environment
Subj: NAVAL AUDIT SERVICE DRAFT REPORT N2008-NIA000-0051.000,
NAVY ANTITERRORISM PROGRAM EXECUTION

Ref: (a) NAVAUDSVC memo 7510/N2008-NIA000-0051.000 of
28 Aug 08

Encl: (1) OPNAV N46 response to NAVAUDSVC draft report number
N2008-NIA000-0051.000 of 28 Aug 08

1. In response to reference (a), enclosure (1) provides the Director, Ashore Readiness response to Finding 1 (Navy Antiterrorism Strategic Plan), Recommendations 2 through 9 in the subject audit report.
2. The audit and our response to the audit recommendations does not contain information we deem "For Official Use Only."
3. The N46 point of contact for this audit is [REDACTED]
[REDACTED] or [REDACTED]
[REDACTED]

FOUO (b)(6)

**Director, Ashore Readiness to Naval Audit Service Draft Report
N2008-NIA000-0051.000**

OPNAV N46

Recommendation 2: Develop controls and implement guidance (in the form of a web-based tracking system) to ensure that regional commands provide oversight by validating installation-level compliance with DoD/Navy AT standards and associated AT Strategic Plan sub-objectives.

Target completion date: 31 March 2009

Response. Concur. N46 will ensure compliance with AT standards and Strategic Plan sub-objectives through establishment of a web based tool for Region oversight. Existing government owned systems, including Antiterrorism Readiness Management System (ARMS) and the AT tracking system developed by Commander, Pacific Fleet have demonstrated the capability required for Regional Commander oversight of Installation compliance. In addition, the SIPR version of CNIC's C4I suite has the capability to incorporate ARMS as has been demonstrated on the NIPR site. Discussion of these systems and possible alternatives including other established hosts/sites including portals will be conducted at the C4I Policy Standards Board in January 2009. Alternatives and the brief for the Policy Standards Board will be developed by the Regional Security Officers who will ultimately be the end users of the system at the December 2008 Force Protection Working Group.

Recommendation 3: Establish the required frequency of installation ATWG meetings; clarify and document in guidance to ensure the requirement is consistently followed by installations.

Target completion date: 31 October 2008

Response. Concur. N46 will coordinate with OPNAV N3AT to ensure ATWG requirements are included and clearly articulated in OPNAV AT policy (3300.53 series) currently under revision. As manager of Ashore Protection OPNAV N46 will ensure installations comply with ATWG frequency requirements established by the DoDI 2000.16 (Para E3.10) requiring the ATWG meet at least semi-annually. N46 has scheduled a meeting with the CNOIVA team leads for the east and west coast for 30 Sep 08 to discuss adding a benchmark for the installation AT assessment to verify

Enclosure (1)

that the ATWG met as required. Additionally, Navy Mission Essential Tasks for Protection will be revised to add a standard for ATWG meeting frequency to allow HQ to track compliance via DRRS/N.

Recommendation 4: Develop an annual AT program review tool, and clarify guidance mandating its use at both the regional and installation level.

Target completion date: 31 August 2009

Response. Concur. N46 will establish the review tool and guidance. Currently N46 is working to determine if the existing JAT can be augmented to satisfy this requirement. Target date for that analysis is 15 Jan 09. N46 will also work with CNIC N3AT/N5 to develop alternatives in lieu of JAT including entries in the existing DRRS-N reporting tool. Target date for completion of that effort is 30 Apr 09.

Recommendation 5: Clarify guidance regarding usage of the Joint Antiterrorism (JAT) guide to develop installation AT Plans and conduct required annual AT assessments and AT Plan reviews. Further, develop an implementation plan to ensure that all CONUS Navy Installation AT personnel have access to the JAT guide.

Target Completion Date: 31 December 2008

Response. Concur. N46 has facilitated the CNIC efforts to implement use of the JAT by Navy installations. Specific implementation guidance for the utilization of the JAT guide will be included in the draft CNIC 5530.XX Security Program Manual, target date is 31 Dec 08 for issuance. CNIC has also begun providing JAT training and assistance to Regional staffs which will reach out to Navy installations. N46 will ensure that installations outside of CNIC enterprise receive same training. CNIC is exploring the possibility of adding the JAT guide to the C4I Suite which is available and monitors 24/7 in Installation, Region, and CNIC Operations Centers.

Recommendation 6: Develop controls and provide oversight to ensure that current guidance regarding CVAMP responsibilities at both the regional and installation level are adhered to, ensuring that identified vulnerabilities are entered within CVAMP, and that installation-level AT related assessments are properly performed, documented, and retained in official files.

Target Completion Date: 30 September 2010

Interim Completion Date: 31 March 2009

Response. Concur. CNIC Instruction 3300.1, Risk Analyzed Mitigation Process (RAMP) (signed 29 Jul 08), directed Regions and Installations to adhere to the process of entering vulnerabilities into CVAMP. Oversight is provided via RAMP, a Commander, Navy Installations Command (CNIC) funded program, whereby Naval Facilities Engineering Service Center (NFESC) engineers physically attend Joint Staff and/or CNO IVA out briefs and assist Navy installations with receipt and disposition of that information. The NFESC engineer will then complete an audit of the CVAMP database 4-6 months after the assessment providing training to the installation CVAMP operator as necessary. It is anticipated that all 78 CNIC installations will receive this service over a three year period. A similar strategy will be utilized to ensure that any remaining Navy installations are evaluated once the majority is completed. By the interim completion date of 31 March 2009, the details and measures of RAMP will become an OPNAV Instruction, most likely included into the existing 3300.53 series, to ensure oversight at the Echelon I level as required and to establish an enduring process beyond the currently funded three year RAMP initiative.

Recommendation 7: Develop an implementation plan to ensure that all CONUS Navy installations have dedicated and reliable SIPRNET access to facilitate use of CVAMP.

Target Completion Date: 31 August 2009

Response. Concur. All installations should have access to SIPRNET which is the only means to access CVAMP. This issue involves resource support from OPNAV N6. Both N46 and N6 have closely coordinated to ensure an optimal solution was found. Strategy for SIPRNET implementation will be developed with an established timeline for logical deployment of the tool to all SIPR/OneNet systems during the period 2-21 Oct 2008, thus resolving access issues by installation AT planners.

Recommendation 8: Develop controls, implement guidance, and provide oversight to ensure that AT personnel develop (and enter into CVAMP) effective POA&Ms for tracking, reporting, and mitigating or eliminating vulnerabilities.

Target Completion Date: 30 September 2010

Interim Completion Date: 31 March 2009

Response. Concur. Referring to the June 2008 CVAMP Periodic Report issued by CNIC reported to the Regions that 85% of the open vulnerabilities entered into CVAMP lacked a design status to mitigate the vulnerability. The RAMP process, referenced in Recommendation 6 is designed to assist installations with determining mitigation strategies. RAMP will also provide a database of past mitigation strategies to vulnerabilities as a reference available to installation Security officers. By the interim completion date of 31 March 2009, the database of past mitigation strategies to vulnerabilities will be available for reference by the installation Security officers. Target date for completion of all installation assessments is 30 Sep 10, the same as recommendation # 6.

Recommendation 9: Develop guidance defining the minimum required elements to be included with POA&Ms.

Target Completion Date: 31 March 2009

Response. Concur. N46 plans to work with NFESC on outlining minimum required information for installation POA&M's. Presently, the CVAMP user guide details minimum information required advancing through the fields in CVAMP to enter data, but there is no ability to verify correctness of the data input into CVAMP by the operator. CNIC will make changes to CNIC Instruction 3300.1 (RAMP) and forward revision to OPNAV N46 for inclusion into policy that will specify POA&M criteria.

~~FOR OFFICIAL USE ONLY~~

~~Use this page as~~

~~BACK COVER~~

~~for printed copies~~

~~of this document~~

~~FOR OFFICIAL USE ONLY~~