PROGRAM REVIEW 4.1

Area of Review: Naval Support Activity Washington (NSAW) Antiterrorism Program
Date: 1-21 Oct 2013

References:

1. DODI 2000.12, DoD Antiterrorism Program, 09 Sep 2013

2. DODI 2000.16, DoD Antiterrorism Standards, 08 Dec 2006

3. SECNAVINST 3300.2B, Department of the Navy (DON) Antiterrorism Program, 28 Dec 2005

4. OPNAVINST F3300.53C, Navy Antiterrorism Program, 26 May 2009

5. USFF AT OPORD 3300-13 dated 01 Jan 2013

6. Navy Tactics, Techniques, and Procedures (NTTP) 3-07.2.1, Antiterrorism, Jun 2010

7. NSAW AT Plan, Mar 2013

Method of Review/Summary:

A review of the NSAW Antiterrorism (AT) Program for execution of and compliance with listed references was conducted. Administrative documents reviewed included drill and training records, local records and instructions associated with the Antiterrorism program, and external AT audits and assessments. Additionally, interviews were conducted with the NSAW Installation Training Officer, the NSAW AT Officer, the NSAW Security Officer, the Naval District Washington (NDW) Training and Readiness Director and the NDW Regional Security Officer.

Deficiencies were identified in program content, execution and assessment. Specific findings were reviewed with the NSAW Security Director, the NSAW Chief of Police, the NSAW Security Officer, and the NSAW AT Officer on 23 Oct 2013.

1. AT Program: The Investigation Team reviewed NSAW's implementation of OPNAVINST F3300.53C (Navy Antiterrorism Program). Specific issues of non-compliance include:

a. An Antiterrorism Threat Working Group (ATWG) does not currently exist at NSAW. DoDI 2000.16 (DoD Antiterrorism Standards) and OPNAVINST F3300.53C require that an ATWG be established and meet at least semi-annually or more frequently, depending upon the level of threat activity, to oversee the implementation of the AT program, to develop and refine AT plans, and to address emergent or

emergency AT program issues. The last ATWG meeting occurred in late 2011 and no minutes from the meeting were available to review.[1]

b. A review of monthly Random Antiterrorism Measure (RAM) schedules for the past year revealed that some RAMs have not been implemented in consideration of local threats as required by DoDI 2000.16, Standard 14. Some appropriate RAMs which have not been implemented (b) (7)(E)
(b) (7)(E)

c. In the past 12 months, NSAW has conducted (b) (7)(E)
(b) (7)(E)
(b) (7)(E) In accordance with DoDI 2000.16, DoD Antiterrorism Standards, random security spot checks of vehicles and persons entering facilities are baseline measures for Force Protection Condition (FPCON) NORMAL (Measure NORMAL 2) and FPCON ALPHA (Measure ALPHA 4). [2]

2. Vulnerability Assessments: The Investigation Team reviewed available NSAW vulnerability assessments and identified a number of deficiencies, including:

a. NSAW has not conducted any annual vulnerability assessments since 2007 other than the Chief of Naval Operations Integrated Vulnerability Assessment (CNOIVA) which was conducted in August 2011 and the Joint Staff Integrated Vulnerability Assessment (JSIVA) conducted in 2007. Annual assessments are required by OPNAVINST F3300.53C and include at a minimum, a validation and update of the local threat assessment, reviewing AT plans, determining the effectiveness of AT training, assessing the physical security of mission critical resources and facilities, and identifying any shortfalls which preclude or limit execution of the AT plan.[3]

b. The CNOIVA conducted in August 2011 identified eleven vulnerabilities and numerous concerns. Four of the eleven vulnerabilities and a number of concerns were repeat findings from the JSIVA conducted by the Defense Threat Reduction Agency (DTRA) in 2007 and were classified as an Operational/Procedural type of deficiency. An Operational/Procedural deficiency is one that can be corrected or mitigated at the installation level with minimal or no commitment of financial resources. Many of these same deficiencies were noted by the Investigation Team.

c. OPNAVINST 3300.53C requires that vulnerabilities identified during the CNOIVA be prioritized, tracked and the actions taken to address the vulnerabilities reported to the Region Commander. Identified vulnerabilities and recommended actions must be submitted into the Core Vulnerability Assessment Management

PROGRAM REVIEW 4.1

Program (CVAMP). The Investigation Team was unable to verify that NSAW's vulnerabilities were being tracked by NSAW in CVAMP due to the transition to a new management program which is in progress Navy-wide. According to the NDW Regional Security Officer, the most recent CVAMP entries in the system for NSAW were from 2007. However, he stated that based upon his discussions with U.S. Fleet Forces Command (USFF) regarding the CVAMP transition, some data may have been lost. NSAW, with the support of NDW, gained access to CVAMP during the week of 14 October and made entries for the vulnerabilities identified during the 2011 CNOIVA.[4]

d. Requests for physical security waivers or exceptions were not submitted for mandatory security requirements identified during the CNOIVA that NSAW cannot meet. OPNAVINST F3300.53C requires that commands accepting a higher risk than established through Navy prescribed AT standards must implement an exception, waiver, and variance program. Exceptions, waivers, variances, or deviations should be submitted to the Director, Shore Readiness (OPNAV(N46)) for endorsement through the region commander. This program provides a management tool for commanding officers and those in the chain of command to review and monitor corrective actions for AT standards which cannot be readily achieved. There is no evidence that corrective actions for shortfalls in AT standards at NSAW are being tracked. (b) (7)(E)

(b) (7)(E)

3. Region Oversight: The Naval District Washington (NDW), as the region commander, is tasked by OPNAVINST F3300.53C to ensure that NSAW develops and implements an effective AT program. NDW is required to conduct an annual review of NSAW's AT program and plans to ensure compliance with AT standards, and is required to verify that the NSAW Commanding Officer conducts an annual vulnerability assessment of the installation. NDW was unable to provide any evidence that these oversight requirements had been fulfilled in the past but reported that a program review was scheduled for October 2013.[6]

---

[1] Summary of Interview (SI) 4.1 with (b) (6), (b) (7)(C), on 8 Oct 2013.
[2] Id.
[3] Id.
[4] SI 4.1 with (b) (6), (b) (7)(C), on 8 Oct 2013 ; and SI 4.5 With (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), on 09 Oct 2013.
[5] Id.
[6] Id.