Admin Officer Guide: Activity Security Manager

DISCLAIMER: The Activity Security Manager role is not limited to only admin personnel and should not be considered an admin function. By instruction, any commissioned officer, chief petty officer and above, and GS-11 and above can be designated as the Activity Security Manager. This Admin Officer Guide is written to assist ANY personnel assigned these duties.

INTRODUCTION

The Activity Security Manager (ASM) is a vital (and required) at the command, and one that some Admin LDOs/CWOs may execute during their career. This position is a trusted agent to the Commanding Officer (CO). It is the ASM's responsibility to oversee this program to assist in the execution of the command's mission. As this program is continuously evolving, you will need to validate all the instructions, messages, and policies during your appointment to this position.

OVERVIEW

Managing the Navy's Personnel Security Program helps to ensure every Sailor is "cleared" and qualified to carry positions of trust within the command. Taking your time, reviewing the references, and understanding what is required is an absolute must while in this position. Review SECNAVINST 5510.30C if you do not know the answer to a question, and if you are still unsure, do not hesitate to reach out to your ISIC (FIRST) or other Admin LDOs/CWOs/SMEs for advice or assistance, before acting or making a final decision.

Admin LDOs/CWOs serving as ASMs could be disadvantaged without the appropriate training. Hence, you should take the opportunity to attend a Security Manager course prior to being designated for this particular position or shortly thereafter. It is a great tool providing additional understanding of the Navy Personnel Security Program (PSP).

ADMIN OFFICER/SECURITY MANAGER ACTION

Per the SECNAVINST 5510.30C, the Activity Security Manager (ASM) roles are listed below:

a. Every command in the Navy and Marine Corps eligible to receive sensitive or classified information is required to designate an ASM (also known as Command Security Manager (CSM)) in writing per DoDm 5200.02, Procedures for the DoD Personnel Security Program of 3 April 2017.

(1) CNO, DNS, CMC, and HQMC PP&O/PS will maintain a copy of subordinate ASM designation letters. Navy Echelon I and II ASMs will maintain a copy of their subordinate ASM designation letters. The designation letter should include the Unit Identification Code, Security Management Office Code, Electronic Questionnaires for Investigations Processing (e-QIP) four-digit identification number and return e-mail address for program management oversight.

b. The ASM will be afforded direct access organizationally to the CO and be organizationally aligned to ensure effective management of the command's security program.

c. The ASM may be assigned full-time, part-time, or as a collateral duty and must be a military officer, senior non-commissioned officer, E-7 or above, a civilian employee, GS-11 or above (or pay band equivalent), with sufficient authority and staff to manage the program for the command. The ASM must be a U.S. citizen and have been the subject of a favorably adjudicated Tier 5 (T5) background investigation (BI) completed within the five years prior to assignment.

d. The ASM must be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc.

e. COs are required to obtain formal training for their ASM. The Naval Security Manager Course offered by the Security Education Training and Awareness Team and the Marine Corps Security Management Course satisfy this requirement.

Duties of the ASM:

a. The ASM is the key in developing and administering the command's PSP. The ASM is the principal advisor on personnel security in the command (except issues specific to SCI, IT, and SAPs unless officially designated for these additional duties and responsibilities) and is responsible to the CO for the security program management.

(1) The duties described here and in reference (d) (DoDINST 2000.16) may be assigned to a number of personnel and may even be assigned to individuals senior to the ASM. However, the ASM remains ultimately responsible to the CO for all program requirements.

(2) The ASM must be cognizant of the command security functions and ensure the security program is coordinated and inclusive of all requirements. Security management may involve direct supervision, oversight, coordination, or a combination thereof, to ensure that those individuals in the command who have security duties are kept abreast of changes in policies and procedures and are provided assistance in solving security problems.

b. The below listed duties apply to every ASM:

(1) Serves as the CO’s advisor and direct representative in matters pertaining to the security of classified information held at the command.

(2) Serves as the CO’s advisor and direct representative in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

(3) Develops written command personnel security procedures, including an emergency plan which integrates emergency destruction drills where required.

(4) Formulates and coordinates the command's security awareness and education program.

(5) Ensures security control of visits to and from the command when the visitor requires and is authorized access to classified information.

(6) Ensures that all PSI are properly prepared and submitted to the DCSA and monitored until completed; and adjudicated by the DoD CAF for all personnel who will handle classified information or will be assigned to sensitive duties.

(7) Ensures that access to classified information is limited to those who are eligible and have the “need-to-know”.

(8) Ensures that PSI, eligibility, and accesses are properly recorded in the JointClearance and Access Verification System (JCAVS) or successor system, and that subordinate commands are properly registered in JCAVS or successor system, as necessary.

(9) Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties

(10) Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

(11) Coordinates with the ISSM on matters of common concern.

(12) Coordinates with the Human Resources Office on matters concerning civilian personnel to include, development of position descriptions, issues involving access to classified information, or assignment to sensitive positions. Uses the Position Designation Tool to determine position designations and to determine if civilian, contractors, or consultants require national security eligibility.

(13) Ensures that all personnel who have had access to classified information who are separating, retiring, or being terminated from employment have completed a Security Termination Statement per Section 4-12. The original statement is filed in the individual's Electronic Service Record or Official Personnel Folder (OPF) and a copy is saved in the command's files.

(14) Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information and records execution of the SF 312 in Defense Information System for Security (DISS). DISS serves as the enterprise-wide solution for personnel security, suitability, and credentialing management for DoD military, civilian, and contractors. DISS replaced the Joint Personnel Adjudication System (JPAS) as the System of Record on March 31, 2021.

SECNAVINST 5510.30C is dated 24 Jan 2020 but applicable when it comes to roles and responsibilities and still the governing reference for the Navy Personnel Security Program regardless of command Type and size. Additionally, there are other references listed in this guide that will assist with other positions and procedures that you assist you as your role as Security Manager. The key factor to this position is to arm yourself with the references and build your command posture and networking to prepare you for success.

REFERENCES

SECNAVINST 5510.30C
DEPARTMENT OF THE NAVY ISSUANCES

SECNAVINST 5510.36B
DEPARTMENT OF THE NAVY ISSUANCES

OPNAVINST 5530.14E
DEPARTMENT OF THE NAVY ISSUANCES

DoDINST 2000.16
DoD Issuances (whs.mil)

DoDM 3305.13 of 14 March 2011
DoD Manual 3305.13, March 14, 2011, Incorporating Change 1, April 26, 2018 (whs.mil)

ALNAV 058/23
mynavyhr.navy.mil/Portals/55/Messages/ALNAV/ALN2023/ALN23058.txt?ver=BBXIcyZDtfmIMmFDb91T7A%3d%3d

This guide is published under the direction of the Administrative Limited Duty Officer/Chief Warrant Officer Board of Directors (BOD) and reflects the BOD's collective recommendations.