OPNAV INSTRUCTION 5510.60N

From: Chief of Naval Operations

Subj: SECURITY REGULATIONS FOR OFFICES UNDER THE COGNIZANCE OF THE CHIEF OF NAVAL OPERATIONS

Ref: (a) OPNAV M-5510.1 of August 2017
     (b) E.O. 13526
     (c) SECNAV M-5510.36 of June 2006
     (d) SECNAV M-5510.30 of June 2006
     (e) DoD Manual 5200.02, Procedures for the Personnel Security Program, 3 April 2017
     (g) SECNAVINST 5239.3B
     (h) USSAN 1-07, United States Security Authority for NATO (USSAN) Instruction, 5 Apr 2007 (NOTAL)

1. **Purpose.** To delineate uniform security policies and responsibilities administered by the Office of the Chief of Naval Operations (OPNAV) Security Office (DNS-34). This instruction is a complete revision and should be reviewed in its entirety. The changes are summarized in subparagraphs 1a through 1d.

   a. Removes the security procedural guidance from the instruction to a stand-alone manual, which is now reference (a).

   b. Adds violations of this instruction by the contract personnel.

   c. Adds action to OPNAV personnel regarding the Cybersecurity Program.

   d. Classified and controlled unclassified information (CUI) information marking requirements.

2. **Cancellation.** OPNAVINST 5510.60M.

3. **Scope and Applicability.** This instruction is the basic guidance for military and civilian personnel, and supporting contractors as delineated by reference (b) under Chief of Naval Operations (CNO) direction. This instruction supplements references (a) and (c) through (g).
4. **Objectives.** To ensure: 1) information classified under the authority of reference (b) is protected from unauthorized disclosure; 2) appointments, assignments, and granting access to classified information or to sensitive duties, are consistent with the interest of policies established in references (a) through (h); and 3) maximum uniformity and effectiveness in the application of security program policies as carried out by the OPNAV security serviced activities.

5. **Command Responsibility and Authority**

   a. Director Navy Staff (DNS) is designated administrator for OPNAV security serviced activities security programs. DNS is supported by the Director of Management (DNS-3) in security administration and enforcement of security programs.

   b. DNS-34 is responsible for the formulation, implementation, and enforcement of security programs including classified and CUI markings, and compliance with directives issued by higher authority. DNS-34 is concurrently designated as the OPNAV security manager under the provisions of references (c) and (d) and security officer under the provisions of reference (a).

6. **Security Organization and Responsibilities**

   a. DNS-34 is the principal advisor for the security program policies within the command and will:

      (1) be responsible to DNS for the protection of classified and CUI information originated by and under the cognizance of the Chief of Naval Operations (CNO);

      (2) monitor command compliance; therefore access to classified information and spaces is authorized and granted to the DNS-34 staff during conduct of assigned duties to include investigations, inspections, and security assist visits;

      (3) concurrently serve as conduit for security direction, guidance, and policy to OPNAV security serviced activities via assigned security coordinators; and

      (4) maintain, update, and approve reference (a).

   b. DNS-34 is assisted in the performance of assigned duties by the staff listed in subparagraphs 6b(1) through 6b(3).

      (1) Head, Personnel Security (DNS-34B)
(a) Implement and monitor the Personnel Security Program to include the approval and initiation of personnel security investigations, granting access to classified information, reviewing investigative reports to determine compliance, and conducting pre-employment screenings.

(b) Ensure personnel assigned to sensitive duties have proper clearance eligibility, access, and personnel security investigations delineated by references (d) and (e).

(2) OPNAV Head, North Atlantic Treaty Organization (NATO) Sub-registry Section (DNS-34C), is responsible for the NATO and Treaty Material Security Program as delineated by reference (h).

(3) OPNAV Head, Information Security and Security Education and Training Section (DNS-34D), is responsible for implementation of the Security Education and Training Program to include obtaining outside training as required, and monitoring training by security coordinators. In addition, DNS-34D conducts inspections and assist visits to provide assistance on compliance with security requirements.

7. Security Inspections and Security Assist Visits
   a. Formal security inspections will be conducted randomly for each OPNAV security serviced activity to review compliance with this instruction and to examine security postures per references (a) through (h). When inspections are completed, a formal report will be generated and forwarded to the activity’s deputy or executive assistant. Deficiencies will be marked as requiring action for a written reply to DNS via DNS-34 covering specific correction. A consolidated annual self-inspection report will be created by DNS-34 and forwarded to Deputy Under Secretary of the Navy for Policy no later than 15 days after the end of each fiscal year.

   b. Security assist visits will be conducted by the OPNAV security inspection team upon request. Assist visits may cover security requirements or specific items as desired by the requesting security coordinator.

8. Action. Personnel assigned to OPNAV security serviced activities must comply with references (a) through (h). Cybersecurity Program for the OPNAV security serviced activities is conducted per reference (a) and reference (g), chapter 16.

9. Violations
   a. Assigned personnel are subject to disciplinary or criminal action under applicable military or Federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.
b. Contractor personnel will be returned to their parent company for properly handling of disciplinary matters.

10. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy (SECNAV) Manual 5210.1 of January 2012.

11. **Review and Effective Date.** Per OPNAVINST 5215.17A, DNS-34 will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, Department of Defense, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. As the instruction nears its 5-year anniversary and it is still required, it will be reissued. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the cancellation is known following the guidance in reference (b).

12. **Forms and Information Management Control**

   a. **Forms.** See appendix C of reference (g) for applicable forms.

   b. **Information Management Control**

      (1) Reporting requirements contained in chapter 1 (paragraphs 4, 5 and 6), chapter 2 (paragraph 4a), chapter 12 (paragraph 6h) and chapter 15 (paragraphs 1a, 1b, 1d, 1e and 2) of reference (g) are exempt from reports control per SECNAV M-5214.1 of December 2005, part IV, subparagraphs 7c, 7g, 7k and 7n.

      (2) Reporting requirement contained in chapter 15 (paragraph 1c) of reference (g) is assigned to OPNAV RCS 5510-6C.

J. G. FOGGO  
Director, Navy Staff

Releasability and distribution:  
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, [https://doni.documentservices.dla.mil](https://doni.documentservices.dla.mil)