DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5510.36A
N09N2
6 October 2006

SECNAV INSTRUCTION 5510.36A

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION SECURITY PROGRAM (ISP) INSTRUCTION

Ref: (a) Executive Order 12958, as Amended, Classified National Security Information, 25 Mar 03
(b) SECNAV M-5510.36, DON Information Security Program Manual, 1 Jul 06
(c) SECNAVINST 5510.30B (Series)
(d) SECNAV M-5510.30, DON Personnel Security Program Manual, 1 Jul 06
(e) DOE Final Rule on Nuclear Classification and Declassification, 10 CFR Part 1045, 22 Dec 97
(f) DoD Directive 5205.7, "Special Access Program (SAP) Policy," 5 Jan 06
(g) DoD Instruction 0-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," 1 Jul 1997
(h) SECNAVINST S5460.3C of 5 Aug 99
(i) DoD Directive 8500.1, "Information Assurance (IA)," 24 Oct 02
(j) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," 6 Feb 03
(k) SECNAV M-5239.1, Department of the Navy Information Assurance (IA) Program, 1 Dec 05
(l) EKMS-1, CMS Policy and Procedures for Navy Electronic Key Management Systems (U), 5 Oct 04
(m) SECNAV M-5210.1, DON Navy Records Management Program, 1 Dec 05

1. Purpose

a. Establish uniform Information Security Program (ISP) policies and procedures.

b. Implement reference (a), which directs agencies to observe the democratic principles of openness and the free flow of information, as well as to enforce protective measures for safeguarding information critical to the national security.

c. Incorporate policies and procedures established by other executive branch agencies.

2. Cancellation. SECNAVINST 5510.36.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

3. Objective. Achieve uniform implementation of ISP policy and procedures throughout the Department of Navy (DON) by pro-active command programs that accomplishes the purpose of reference (b). Further, this instruction, and references (b) through (d), complement each other and have been coordinated to achieve compatibility.

4. Applicability and Scope

a. This instruction and the accompanying policy and procedural manual, reference (b), encompass all classified national security information classified under Executive Order 12958, as Amended, and predecessor orders, and special types of classified and controlled unclassified information.

b. This instruction applies to all DON commands and to all military and civilian personnel, assigned to or employed by any element of the DON, and includes cleared contractor visitors working under the purview of a commanding officer. Personnel are individually responsible for compliance. This instruction establishes the minimum standards for classifying, safeguarding, transmitting and destroying classified information as required by higher authority.

5. Roles and Responsibilities

a. The Secretary of the Navy (SECNAV) is responsible for implementing an ISP per the provisions of Executive Orders, public laws, and directives issued by the National Security Council (NSC), Department of Energy (DOD), Department of Defense DOD), Director National Intelligence (DNI), and other agencies regarding the protection of classified information.

b. The Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N)/ DIRNCIS) is designated by the SECNAV as the DON senior agency official under reference (a) and the DON Restricted Data (RD) management official under reference (e).

(1) The CNO (N09N) is responsible to the SECNAV for establishing, directing, and overseeing an effective DON ISP, and for implementing and complying with all directives issued by higher authority. This responsibility includes:

(a) Formulating policies and procedures, issuing directives, and monitoring, inspecting, and reporting on the status of the ISP in the DON.

(b) Implementing the National Industrial Security Program within the DON.

(c) Ensuring that persons with access to RD (including Critical Nuclear Weapons Design Information) and Formerly Restricted Data (FRD) information are trained on appropriate classification, handling, and declassification procedures; and serving as the primary point of contact for coordination with the DOE Director of Declassification on RD and FRD classification and declassification issues.

(d) Serving as primary ISP liaison with the Information Security Oversight Office, Office of the Secretary of Defense and other DoD components and Federal agencies.

(e) Maintaining a World Wide Web page that provides information related to the DON Information and Personnel Security Program (PSP). The CNO Web page may be found at www.navysecurity.navy.mil.

(2) The CNO (N09N) is also responsible for establishing, administering, and overseeing the DON Personnel Security Program, and issuing personnel security policy and procedures in reference (c).

(3) The DIRNCIS is responsible for investigative, law enforcement, physical security, technical surveillance countermeasures, and counterintelligence (CI) programs within the DON.

c. The Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director for Information and Personnel Security Programs (NCIS-24E) provides staff support for the CNO (N09N) functions and responsibilities described in paragraph 5b.

d. The Director, Navy International Programs Office (Navy IPO) is responsible to the Assistant Secretary of the Navy, Research Development and Acquisition (ANS(RD&A)) for implementing policies and managing DON participation in international efforts concerning ASN(RD&A). The Director makes release determinations for disclosure of classified and controlled unclassified information to foreign governments and organizations in compliance with national disclosure policy and manages certain personnel exchange programs with foreign governments.

e. The Director of Naval Intelligence (DNI) (CNO (N2)) is a Senior Official of the Intelligence Community (SOIC) and administers the Sensitive Compartmented Information (SCI) program for the Navy, including non-Service DON entities.

(1) The Office of Naval Intelligence (ONI) is responsible for the security management, implementation, and oversight of SCI security programs on behalf of CNO (N2).

(2) The Director, Security and Corporate Services (ONI-05) is the Special Security Officer for the DON (SSO Navy) and is

designated as the Cognizant Security Authority (CSA). As CSA, SSO Navy is responsible for implementing SCI security policy and procedures and performs management and oversight of the Department's SCI security program.

f. The Director of Intelligence of the Marine Corps is a SOIC and administers the SCI program for the Marine Corps.

g. The Director, Special Programs Division (N89) is designated as the DON Special Access Program (SAP) coordinator and is responsible for the management of the DON SAP Central Office, and for coordinating SAP approval, administration, support, review, and oversight per references (f), (g), and (h).

h. The Department of the Navy, Chief Information Officer (CIO) is responsible for DON policies and implementation of the DoD Information Assurance program under references (i) and (j), respectively. The DON CIO issues reference (k), and is also responsible for Information Management and Information Management Resource Technology matters.

i. The Commander, Naval Network and Warfare Command, Security Directorate, as the designated Special Security Officer is responsible for signals intelligence activities and for administration of SCI programs within the DON cryptologic community.

j. The Director, COMSEC Material System (DCMS) administers the DON CMS program and acts as the central office of records for all DON CMS accounts per reference (l).

k. The Commandant of the Marine Corps (CMC) administers the DON ISP within the U.S. Marine Corps. Designated functions are performed by specific organizations within the Headquarters, Marine Corps:

(1) CMC Director, Administration and Resources management (Code ARS) is responsible for implementation of CI and human intelligence programs and the ISP. All requirements for policy waivers, interpretations and exceptions will be reviewed by the CMC (Code ARS).

(2) CMC Special Security Officer/Special Intelligence Communications Branch (Code IOS) for the U.S. Marine Corps, is responsible for guidance and implementation of SCI programs.

l. The Commanding Officer (used as a generic term for the head of any DON command and includes commander, commanding general, director, officer in charge, etc.) is responsible for the effective management of the ISP within the command. Authority delegated by this instruction to a commanding officer may be further delegated unless specifically prohibited.

6. Action. Each DON commanding officer shall establish and conduct an ISP in compliance with this instruction and reference (b).

7. Violations of this Instruction.

(a) Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this instruction.

(b) Civilian employees are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this instruction.

8. Summary of Changes. Overarching policy is stated in this instruction, and specific policy and procedures are set forth in reference (b).

9. Records Disposition. Disposition requirements for records related to the ISP are based upon schedules approved by the Archivist of the United States and listed in reference (m).

Donald C. Winter
Secretary of the Navy

Distribution:
Electronic only, via Navy Directives Website
http://neds.daps.dla.mil

MARCOR PCN 21600401100