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

SECNAVINST 5510.37
DUSN PPOI
AUG -8 2013

SECNAV INSTRUCTION 5510.37

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INSIDER THREAT PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) DON Insider Threat Program Senior Executive Board (DON ITP SEB)
(3) Responsibilities

1. Purpose. To establish the Department of the Navy Insider Threat Program (DON ITP) per references (a) through (u), promulgate policy, assign responsibilities and institute the DON ITP Senior Executive Board (DON ITP SEB).

2. Applicability. Applies to all personnel, employed by, detailed or assigned to the DON, including civil servants, members of the active and reserve components of the U.S. Marine Corps and U.S. Navy; experts or consultants performing services for the DON through a personnel appointment or a contractual arrangement; industrial or commercial contractors, licensees, certificate holders, or grantees, including subcontractors.

3. Accountability. All DON personnel are responsible for reporting activity that could cause harm to national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

4. Background. As a result of unauthorized disclosures of classified information that damaged national security and violent acts which resulted in loss of life and damage to operational resources, the President directed the establishment of Insider Threat Programs (ITP) across the Executive Branch and identified minimum ITP standards, reference (a).

5. Policy

a. The DON shall establish an integrated set of policies and procedures to deter, detect, and mitigate insider threats before damage is done to national security, personnel, resources and/or capabilities. The DON shall:

(1) Ensure existing and emerging insider threat training and awareness programs are developed, updated and implemented.

(2) Enhance technical capabilities to monitor user activity on all systems in support of a continuous evaluation.

(3) Leverage antiterrorism/force protection (AT/FP), counterintelligence (CI), human resources (HR), information assurance (IA), law enforcement (LE), security and other authorities to improve existing insider threat detection and mitigation efforts.

(4) Detect, mitigate and respond to insider threats through standardized processes and procedures. DON ITP response shall include, but is not limited to, adjudicative, investigative and other administrative actions.

(5) Ensure legal, civil and privacy rights are safeguarded.

(6) Promote the awareness and use of employee assistance programs to enhance interventions for employees in need.

b. Establish a DON ITP Senior Executive Board (SEB), see enclosure (2), to review DON ITP strategic goals, approve program implementation, approve standardized procedures, and develop prioritized resource recommendations for the Secretary of the Navy (SECNAV).

6. Responsibilities. See enclosure (3).

7. Insider Threat Definition. Per reference (p), an insider threat is a person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities. The term

kinetic can include, but is not limited to, the threat of harm from sabotage or workplace violence.

8. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

RAY MABUS

Distribution:
Electronic only, via Department of the Navy Issuances Web site http://doni.documentservices.dla.mil/

REFERENCES

(a) Presidential Memorandum of 21 November 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
(b) E.O. 13587
(c) E.O. 12333, as amended
(d) E.O. 13526
(e) E.O. 12968, as amended
(f) E.O. 10450, as amended
(g) Intelligence Community Directive 700, Protection of National Intelligence of 7 June 2012
(h) Intelligence Community Policy Guidance 704-1, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, of 2 October 2008
(i) Intelligence Community Standard 500.27, Collection and Sharing of Audit Data of 2 June 2011 (NOTAL)
(j) Intelligence Community Standard 700-2, Use of Audit Data for Insider Threat Detection of 2 June 2011
(k) Committee on National Security Systems (CNSSP) 22, Information Assurance Risk Management for National Security Systems of January 2012
(l) Committee on National Security Systems Directive (CNSSD) 504, Protecting National Security Systems from Insider Threat of Jan 2012 (NOTAL)
(m) DoD Instruction 2000.12 of 1 March 2012
(n) DoD Instruction 2000.26 of 1 November 2011
(o) DoD Instruction 5210.91 of 12 August 2010
(p) DoD Instruction 5240.26 of 4 May 2012
(q) DoD Directive 5240.06 of 17 May 2011
(r) DoD Directive 8500.01E of 24 October 2002
(s) SECNAVINST 5211.5E, Department of the Navy (DON) Privacy Program, of 28 December 2005
(t) SECNAV M-5510.30, Department of the Navy Personnel Security Program Manual of June 2006
(u) SECNAV M-5510.36, Department of the Navy Information Security Program Manual of June 2006

DON INSIDER THREAT PROGRAM SENIOR EXECUTIVE BOARD (DON ITP SEB)

1. The DON ITP SEB shall:

a. Submit a DON ITP SEB charter for approval by the Under Secretary of the Navy (UNSECNAV) bi-annually.

b. Exercise oversight, management, and review over all DON ITP activities;

c. Receive reports from the DON ITP annually, or as deemed necessary by the chair;

d. Review and act on recommendations of the Naval Inspector General (NAVINSGEN) related to DON ITP activities; and

e. Meet semi-annually or as required by the chair.

f. Charter working groups as required to research and recommend courses of action for the DON ITP SEB to consider/approve. Working group charters will have sunset clauses.

2. DON ITP SEB Membership

a. The DON ITP SEB shall be chaired by the Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration (DUSN PPOI). As the chair, the DUSN PPOI shall determine a quorum and may invite other officials to consider individual issues for which special expertise is required. Attendance shall be by Principal and Advisory Members only, except by permission of the chair.

b. Principal Members.

(1) Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)).

(2) Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)).

(3) Department of the Navy/Assistant for Administration (DON/AA).

(4) Department of the Navy Chief Information Officer (DON CIO).

(5) Director, Naval Criminal Investigative Service (DIR NCIS).

(6) Commandant of the Marine Corps' 3 star representative.

(7) Chief of Naval Operations' three star representative.

(8) Director, Department of the Navy Special Access Programs Central Office.

c. Advisory Members.

(1) DON General Counsel.

(2) Deputy Commandant for Manpower and Reserve Affairs.

(3) Deputy Commandant for Plans, Policies and Operations.

(4) Department of the Navy Deputy Chief Information Officer for the United States Marine Corp.

(5)Deputy Chief of Naval Operations for Manpower, Personnel and Education (N1).

(6) Deputy Chief of Naval Operations for Information Dominance (N2/N6).

(7) Deputy Chief of Naval Operations for Operations, Plans, and Strategy (N3/N5).

(8) Deputy Chief of Naval Operations for Fleet Readiness and Logistics (N4).

(9) Surgeon General of the Navy.

(10) Staff Judge Advocate to the Commandant of the Marine Corps.

(11) Judge Advocate General of the Navy.

(12) Deputy Assistant Secretary of the Navy for Civilian Human Resources.

3. Administrative Support. The Senior Director for Security, or a designated delegate, will serve as executive secretary of the DON ITP SEB and oversee any chartered DON ITP SEB working groups.

4. Record of Proceedings. The DON ITP SEB executive secretary shall prepare and forward to DUSN PPOI for approval a record of the DON ITP SEB proceedings, and maintain the original signed copies per SECNAV M-5210.1.

RESPONSIBILITIES

1. The SECNAV is responsible for establishing and operating the DON ITP in accordance with reference (b).

2. The DUSN PPOI, under the authority, direction, and control of the SECNAV and UNSECNAV, shall:

a. Serve as the DON senior executive responsible for DON ITP management, accountability, and oversight decisions, and resource recommendations to the SECNAV.

b. Develop and promulgate comprehensive DON ITP policy to be approved by the SECNAV.

c. Ensure standardized processes are developed and implemented which DON ITP nodes will use to centrally gather, integrate, analyze and respond to information indicative of a potential insider threat.

d. Ensure procedures and agreements are established to allow appropriate DON ITP entities access to information, pograms and systems to support program implementation.

e. Establish guidelines for components to directly refer and directly receive information from the appropriate DON ITP entity.

f. Ensure DON ITP timely access to appropriate intelligence and counterintelligence products reporting threats to the DON.

g. Ensure policies exist and are enforced for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

h. Establish policy to subject personnel assigned insider threat detection duties to continuous evaluation to ensure DON ITP data is not misused and that tactics, techniques and procedures are not compromised.

i. Develop and submit to the SECNAV an implementation plan for establishing the DON ITP and annually thereafter a DON ITP progress report. At a minimum, the annual reports shall

document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations for program improvement, and major impediments or challenges.

j. Ensure DON ITP is implemented in accordance with applicable laws, policies, regulations and orders, including, but not limited to, the need for a Privacy Impact Assessment (PIA) and System of Records Notice (SORN) prior to the retention of any DON ITP records in a database.

k. Ensure the establishment of guidelines for the retention of records necessary to complete assessments required by reference (b).

l. Facilitate oversight inspections of the DON ITP by the Office of the Naval Inspector General and other cleared officials.

m. Classify DON ITP information in accordance with National ITP classification guidance.

n. Chair the DON ITP SEB.

3. Senior Director for Security shall:

a. Provide staff support to the DUSN PPOI in carrying out the above assigned duties.

b. Serve as the DON ITP SEB Executive Secretary.

c. Charter working groups as required to research and recommend courses of action for the DON ITP SEB to consider.

4. Department of the Navy General Counsel shall:

a. Provide legal advice to DON clients to assist them in carrying out their responsibilities under this instruction.

b. Be an advisory member of the DON ITP SEB.

c. Provide legal advisors to DON ITP chartered working groups.

5. DON CIO shall:

a. Review and update IA publications as necessary to ensure DON organizations coordinate DON ITP access to required data streams, in accordance with applicable laws, policies, regulations and orders.

b. Enhance accessibility standardization of existing mechanisms (i.e. tip lines, hotlines, on-line reporting etc.) for anonymous reporting of suspected insider threat activities or behaviors.

c. Ensure, in coordination with Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA), DON organizations design, develop, deploy, and operate technology-enabled techniques on all DON networks to discover and monitor user activities that may indicate insider threat activity.

d. Develop and maintain a standardized acceptable use policy that guides user behavior when accessing and using DON information systems and or networks.

e. Ensure all DON network service level agreements include provisions for DON ITP access to network user activities.

f. Ensure information technologies deployed in support of DON ITP are accredited and maintain accreditation.

g. Ensure all DON Insider Threat policies include the appropriate reference to security controls the systems/networks must have in place to support the policy.

h. Ensure requirement for standardized classified and unclassified network banners and mandatory signed user agreements informing users that their activity on the network is being monitored for lawful authorized purposes and are up to date with current policies.

i. Provide prioritized planning guidance to the Services to ensure they plan, program and budget the resources to carry out DON ITP IA related activities.

j. Be a member of the DON ITP SEB.

k. Provide IA representatives to DON ITP chartered working groups.

6. Director, NCIS shall:

a. Provide CI/Insider Threat Awareness and Reporting training in accordance with reference (q).

b. Receive CI/LE referrals from the DON ITP for further analysis and appropriate CI/LE response.

c. Consistent with any disclosure restrictions related to ongoing ITP investigations, provide periodic updates as appropriate regarding the status of accepted referrals to the DON ITP.

d. Provide information to the DON ITP that does not meet CI/LE response thresholds for further analysis and action as appropriate.

e. Consistent with legal and policy disclosure restrictions, provide information from polygraph examinations to inform the appropriate DON IT entity.

f. Plan, program and budget the resources to carry out DON ITP CI/LE activities.

g. Be a member of the DON ITP SEB.

h. Provide CI/LE representatives to DON ITP chartered working groups.

7. ASN (M&RA) shall:

a. Ensure that military and civilian manpower policies are updated, as required, to reflect DON ITP information sharing requirements.

b. Ensure DON ITP access to all relevant DON HR databases and files to include, but not limited to, personnel files, payroll and voucher files, official travel files, outside work, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

c. Provide a standardized method for identifying the DON ITP Training requirement for all employees, verify completion of the training and report training results to the DON ITP annually.

d. In coordination with the DON CIO and the General Counsel, ensure agreements signed by all employees acknowledging that their activity on any DON network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security or administrative proceeding. Agreements shall be made a part of the individual's permanent record and shall be executed upon entry-on-duty.

e. Collaborate with OPM, Marine Corps and Navy Recruiting Commands and Office of Civilian Human Resources to develop enhanced pre-employment screening tools to identify insider threat concerns.

f. Ensure Office of Civilian Human Resources:

(1) Provides awareness briefings to new employees concerning employee assistance programs and other resources available to reduce situations that affect employee performance.

(2) Receives referrals from the appropriate DON ITP entity for further analysis and appropriate response.

(3) Provides the appropriate DON ITP entity with information that does not meet the HR response threshold.

(4) Plans, programs and budgets the resources necessary to carryout DON ITP HR activities.

g. Be a member of the DON ITP SEB.

h. Provide HR representatives to DON ITP chartered working groups.

8. ASN (RD&A) shall:

a. Ensure that contracts awarded by the DON incorporate provisions that support enforcement of the DON ITP policies set forth by DUSN PPOI and consistent with Federal Acquisition

Regulations (FAR) and Defense Federal Acquisition Regulations Supplement (DFARS).

b. Ensure contracting officers are trained on the need to enforce DON ITP requirements in all contracts involving access to information, operation of networks owned by the DON, and the DON ITP training and reporting requirements.

c. Be a member of the DON ITP SEB.

d. Provide RDA representatives to DON ITP chartered working groups.

9. The Office of the Naval Inspector General shall inspect the DON ITP as the Naval Inspector General deems appropriate in accordance with applicable laws, policies, regulations and orders.

10. Commandant of the Marine Corps (CMC), Chief of Naval Operations (CNO) and the DON/AA shall:

a. Build and maintain a DON insider threat analytic and response capability to gather, integrate, review, assess, and respond to anomalous information derived from AT/FP, CI, IA, HR, LE, security, user activity monitoring, and other sources as necessary and appropriate.

(1) Collaboratively develop the process by which DON ITP nodes will centrally gather, integrate, analyze and respond to information indicative of a potential insider threat

(2) Ensure capability developed includes all personnel, employed by, detailed or assigned to the DON, including civil servants, members of the active and reserve components of the U.S. Marine Corps and U.S. Navy; experts or consultants performing services for the DON through a personnel appointment or a contractual arrangement; industrial or commercial contractors, licensees, certificate holders, or grantees, including subcontractors.

(3) Ensure DON standardized ITP practices, procedures, and information technology systems, applications, and/or database use mandates are employed at every echelon conducting DON ITP activities.

b. Document each insider threat matter reported and response action taken and ensure timely resolution of each matter.

c. Ensure personnel assigned to insider threat duties, regardless of service affiliation, receive standardized integrated training in:

(1) CI and security fundamentals including applicable legal issues;

(2) Procedures for conducting insider threat inquiry action(s);

(3) Applicable laws, policies, regulations and orders regarding the gathering, integration, retention, safeguarding and use of records and data (including the consequences of misuse of such information), including, but not limited to laws, policies, regulations and orders regarding civil liberties and privacy.

(4) CI and LE investigative referral requirements to NCIS, as well as other policy or statutory requirements that require referrals to security, NAVINSGEN or other authorities.

d. Coordinate DON ITP access to required data streams in accordance with applicable laws, policies, regulations and orders.

e. Design, develop, deploy, and operate technology-enabled techniques on all DON networks to discover and monitor user activities that may indicate insider threat activity.

f. Ensure all network service level agreements include provisions for DON ITP access to network user activities.

g. Deploy and maintain accredited information technologies in support of the DON ITP.

h. Ensure Security Officials at every echelon:

(1) Provide security awareness briefings to all personnel assigned.

(2) Receive referrals from the appropriate DON ITP entity for further analysis and appropriate response.

(3) Provide information to the appropriate DON ITP entity that does not meet the security response threshold.

(4) Plan, program and budget the resources necessary to carryout DON ITP related activities.

i. Plan, program and budget the resources to carryout DON ITP activities.

j. Assign appropriate three star representatives to the DON ITP SEB.

k. Provide appropriate service representatives to DON ITP chartered working groups upon request.

11. Surgeon General of the Navy shall:

a. Provide medical and psychological expertise to the appropriate DON ITP entity to advise on clinical issues relevant to the behaviors observed.

b. Identify and provide the appropriate DON ITP entity access to information as authorized, in accordance with applicable laws, policies, regulations and orders, including but not limited to the Health Insurance Portability and Accountability Act.

c. Plan, program and budget the resources to carry out DON ITP medical and psychological activities.

d. Be an advisory member of the DON ITP SEB.

e. Provide medical and/or psychological representatives to DON ITP chartered working groups as required.

12. Chief of Chaplains shall:

a. Identify information received by Chaplains that may permissibly be provided to the appropriate DON ITP entity.

b. Develop and implement a process for providing unprivileged communications to the appropriate DON ITP entity.