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

SECNAVINST 5510.37A
DUSN
28 Oct 2019

SECNAV INSTRUCTION 5510.37A

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INSIDER THREAT PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Definitions
(3) Responsibilities

1. Purpose. To establish the Department of the Navy Insider Threat Program (DON ITP) per references (a) through (r), promulgate policy, define governance, and assign responsibilities.

2. Cancellation. SECNAVINST 5510.37.

3. Definitions. See enclosure (2).

4. Background. As a result of unauthorized disclosures of classified information that damaged national security, the President directed the establishment of ITPs across the Executive Branch, reference (a), and identified minimum ITP standards to be upheld, reference (b). The DON program will, hereinafter, be referred to as the DON ITP. Reference (c) expanded the definition of “insider threat” to include commission of a destructive act, which may include physical harm to another in the workplace.

5. Applicability

a. The Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), and the Commandant of the Marine Corps (CMC), and all U.S. Navy, U.S. Marine Corps installations, commands, activities, field offices, and all other organizational entities within the DON.

b. For the purpose of this instruction, “DON employee” or “employee” will refer to military personnel, civilian personnel,

and contractors. A more descriptive definition is available in enclosure (2).

c. This instruction does not supersede:

(1) Authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information and special access programs for intelligence as directed by reference (d).

(2) Applicable law, regulation, and policy governing access to, or dissemination of, Law Enforcement (LE), LE sensitive, or classified LE information.

(3) Suspicious activity reporting and dissemination requirements as outlined in reference (e).

(4) Applicable law, regulation, and policy governing Counterintelligence (CI) and other intelligence activities.

(5) Requirements to refer information on criminal or CI allegations, or suspected criminal or CI allegations involving persons affiliated with the Department of Defense (DoD) or any property or programs under the control or authority of the DON to Naval Criminal Investigative Service (NCIS) as expeditiously as possible. Referral to NCIS shall not be delayed for any improper purpose, to include adjudicative, investigative, and other administrative actions for matters that fall within the jurisdiction of NCIS pursuant to references (f) and (g).

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

a. Ensure existing and emerging insider threat training and awareness is provided to all DON personnel, or other insiders, who have access to DON resources.

b. Enhance technical capabilities for User Activity Monitoring (UAM) on all DON classified information networks. This policy does not prohibit UAM on unclassified networks.

c. Establish a single DON Insider Threat Analytic Hub, hereafter referred to as DON Insider Threat Hub, which will serve as an integrated capability to monitor and audit information for insider threat detection and mitigation. This capability will gather, integrate, review, assess, and respond to information derived from the following areas: Antiterrorism/Force Protection risk management (AT/FP); CI; civilian and military personnel management; Cybersecurity (CS); LE; Security; Inspector General (IG); the monitoring of user activity on classified DON information networks; Prevention, Assistance, and Response (PAR) capabilities and framework; continuous evaluation and other sources as necessary and appropriate to improve existing insider threat detection and mitigation efforts.

d. Detect, mitigate, and respond to insider threats through standardized processes and procedures. DON responses will include, but are not limited to, adjudicative, investigative, and other administrative actions.

e. Ensure the collection, use, maintenance, and dissemination of information critical to the success of the DON ITP complies with all controlling law, regulation, and policy including those regarding whistleblower, civil liberties, and privacy protection.

f. Implement a PAR or PAR-like capability as described in reference (m). Synchronize these capabilities with those residing in the DON ITP.

g. Utilize the DON Security Enterprise Executive Committee (DON SE EXCOM), reference (h), to review DON ITP strategic goals, approve program implementation, approve standardized procedures, and develop prioritized resource recommendations for the SECNAV.

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

8. Objectives

a. Network monitoring and auditing. Monitoring and auditing capabilities must be employed to support insider threat detection and mitigation efforts in accordance with reference (q), applicable law, regulations, and policy. These capabilities will be integrated into the overall insider threat detection and mitigation process. Capabilities must periodically be reviewed and improved in order to meet current and future DON mission requirements and to proactively incorporate best practices to prevent and detect anomalous activity.

b. Information sharing. The timely sharing of information is integral to the DON ITP. Pertinent information from CI, CS, Security, PAR capabilities, LE, civilian and military personnel management sources, and UAM will be shared with ITP personnel. Information sharing policies and procedures must comply with controlling law, regulation, and policy, including reference (q) and reference (r). Additionally, the DON ITP must share insider threat information with the DoD Insider Threat Management and Analysis Center (DITMAC) using the DON Insider Threat Hub in accordance with reference (i). Information acquired, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power must be referred to the Federal Bureau of Investigation (FBI) through the NCIS in accordance with reference (j).

c. Training and Awareness. DON ITP personnel will receive training in accordance with the criteria annotated in reference (b).

d. Insider Threat Reporting and Response. Reporting behaviors of concern among the stakeholders, primarily the stakeholders listed in enclosure (3), is necessary to determine the severity of the threat and appropriate response. Procedures must be in place in order for DON ITP personnel to collect necessary and relevant information, analyze and appropriately respond to mitigate the threat.

9. Responsibilities. See enclosure (3).

10. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to reference (k) and the records disposition schedules found on the Directives and Records Management Division portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records of disposition schedules, please contact your local Records Manager or the DRMD program office.

11. Information Management Control. The reporting requirements contained in enclosure (3), paragraphs 16k is exempt from information management control, per reference (s), Part IV, paragraph 7o.

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni.

REFERENCES

(a) E.O. 13587
(b) Presidential Memorandum of 21 November 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
(c) NDAA for Fiscal Year 2017, Section 951
(d) E.O. 12333
(e) DoD Instruction 2000.26 of 23 September 2014
(f) SECNAVINST 5430.7R
(g) SECNAVINST 5430.107A
(h) SECNAVINST 5500.36A
(i) UNSECDEF for Intel Memo of 29 December 2016, Reporting Information to the Department of Defense Insider Threat Management and Analysis Center
(j) 50 U.S.C. §3381
(k) NARA 45, Insider Threat Program Records, National Archives and Records Administration
(l) DoD Directive 5205.16 of 30 September 2014
(m) DEPSECDEF Memo of 02 February 2017, Final Implementation Actions of Fort Hood Recommendations: Managing Risk of Potentially Violent Behavior Through Prevention, Assistance, and Response Capabilities
(n) DoD Directive 5240.06 of 17 May 2011
(o) SECNAVINST S5460.3H
(p) SECNAVINST 5200.35G
(q) 5 U.S.C. §552a
(r) 5 U.S.C. §2302b
(s) SECNAV M-5214.1

DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction:

1. Classified Information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

2. Employee. A person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

3. Insider. Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

4. Insider Threat. As defined in reference (c), a threat presented by a person who:

a. Has or once had authorized access to information, a facility, network, person, or resource of the department; and

b. Wittingly, or unwittingly, commits:

(1) An act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or

(2) A destructive act, which many include physical harm to another in the workplace.

5. Insider Threat Hub. An insider threat analytic and response capability/activity which gathers, integrates, reviews, assesses, and responds to information derived from CI, Security,

CS, Human Resources, LE, IG, UAM, and other sources as necessary and appropriate.

6. PAR Capabilities. A network of multi-disciplinary efforts, each led by a functional expert and normally resident on or available at the installation level, that commanders and their equivalent civilian leaders can use to aid them in identifying the level of risk that violent behavior poses to DON personnel, organizations, installations, or separate facilities, and in developing risk-response recommendations to mitigate or remediate this risk.

RESPONSIBILITIES

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

2. The Under Secretary of the Navy (UNSECNAV) is responsible for the oversight, management, and compliance of DON ITP, primarily exercised through the office of the Deputy Under Secretary of the Navy (DUSN).

3. Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN (M&RA)) will:

a. Securely provide ITP personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters involving both military and civilian DON employees. Such access and information includes, but is not limited to, personnel files, payroll and voucher files, official travel files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat incidents and anomalous behavior.

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

c. Establish, consistent with applicable law, regulation, and policy, procedures for access requests by DON ITP personnel involving particularly sensitive or protected information. Ensure procedures are consistent with privacy laws, civil liberties, and regulations.

d. Ensure uniformed members within the DON have access to assistance programs and other resources available to avoid or mitigate situations that affect employee performance.

e. In coordination with the Department of the Navy Chief Information Officer (DON CIO), the General Counsel (GC) and the Judge Advocate General (JAG), ensure agreements signed by all employees acknowledging that their activity on DON information networks, to include portable electronic devices, is subject to

monitoring and could be used against them in a criminal, security, or administrative proceeding.

f. Collaborate with Office of Personnel Management, Marine Corps and Navy Recruiting Commands, and Office of Civilian HR to develop enhanced pre-employment screening tools to identify insider threat concerns.

g. Ensure Office of Civilian Human Resources:

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

(2) Receives referrals from the DON Insider Threat Hub for further analysis and appropriate response.

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

h. Serve as a member of the DON SE EXCOM as described in reference (h).

i. Provide HR representative(s) to DON ITP chartered working groups.

4. Assistant Secretary of the Navy (Research Development and Acquisition (ASN (RD&A)) will:

a. Ensure that contracts awarded by the DON include the appropriate Federal Acquisition Regulations and Defense Federal Acquisition Regulations Supplement clause.

b. Ensure Security Managers 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. Serve as a member of the DON SE EXCOM as described in reference (h).

d. Provide ASN (RD&A) representative(s) to DON ITP chartered working groups.

5. DON GC will:

a. Provide legal advice and review on subject matters listed in this instruction.

b. Serve as a member of the DON SE EXCOM as described in reference (h).

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

6. The DUSN, under the authority, direction, and control of the UNSECNAV, will serve as the DON Insider Threat Senior Official responsible for management and oversight of the DON ITP and provide resource recommendations to the UNSECNAV. As the Senior Official, the DUSN will:

a. Ensure procedures and agreements are established to allow appropriate DON ITP stakeholders access to information, programs and systems necessary to support program implementation.

b. Ensure the DON ITP is developed in accordance with references (a),(b), and (l) and in consultation with the DON GC, JAG, Staff Judge Advocate to CMC, and civil liberties and privacy officials, for matters under their cognizance, so that all ITP activities, to include training, are conducted in accordance with applicable law, regulation, and policy.

c. Establish a single DON central insider threat capability that analyzes information from all relevant sources to identify insider threat concerns and initiate responses. This capability is the DON Insider Threat Hub.

d. Ensure the DON ITP is implemented in accordance with applicable laws, policies, regulations and orders, including, but not limited to, the requirements related to a Privacy Impact Assessment and System of Records Notice prior to the retention of any DON ITP records in a database.

e. Establish oversight procedures to ensure proper handling, use, and retention of records and acquired data.

Ensure that access to such records and data is restricted to personnel who require the information to perform their authorized functions. These procedures will include the retention of records and documents necessary to complete the assessments required by reference (b).

f. Facilitate oversight reviews with the Office of Naval Inspector General to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy, and civil liberties protections.

g. Ensure the implementation of a PAR or PAR-like capability as described in reference (m).

h. Designate the DON ITP as an Assessable Unit within the DUSN Managers' Internal Control Program (MICP) in accordance with reference (p).

i. Serve as the chair of the DON SE EXCOM (reference (h)).

7. CIO will:

a. Review and update CS publications, as necessary, to require that DON classified network owners plan and conduct UAM on DON classified networks and provide support for DON ITP access to required data streams, in accordance with applicable law, regulation, and policy.

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 the ASN (RD&A), DON organizations design, develop, deploy, and operate technology-enabled techniques on DON classified networks to discover and monitor user activities or anomalous behavior 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 networks.

e. Update DON CIO policy to support regular and timely access to network and system audit information for ITP personnel to support the identification, analysis, and resolution of insider threat issues.

f. Provide prioritized planning guidance to the Navy and Marine Corps to assist in the planning, programing, and budgeting of resources to carry out DON ITP CS related activities as appropriate.

g. Ensure information technologies deployed in support of DON ITP are authorized on the network and maintain that authorization.

h. Ensure all DON CS policies include the appropriate reference to security controls the systems/networks must have in place to support the policies.

i. Ensure the requirement for standardized DON network banners and mandatory signed user agreements inform users that their activity on the network is being monitored for lawful authorized purposes and is up to date with current policies.

j. Serve as a member of the DON SE EXCOM as described in reference (h).

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

8. Director, NCIS as the Senior Official for Criminal Investigations and CI, will:

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

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

c. Submit all DON referrals to the FBI of any information, regardless of origin, which indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power pursuant to references (j).

d. Consistent with law, regulation, and policy, including disclosure restrictions related to ongoing CI/LE investigations, provide periodic updates based on significant milestones or as appropriate regarding the status of accepted referrals to the DON ITP.

e. Provide information to the DON Insider Threat Hub that does not meet CI/LE response thresholds for further analysis and action as appropriate.

f. Consistent with disclosure restrictions, provide information from polygraph examinations to inform the DON Insider Threat Hub.

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

h. Program and conduct UAM on NCIS classified networks.

i. Serve as a member of the DON SE EXCOM as described in reference (h).

j. Provide CI/LE representative(s) to DON ITP chartered working groups.

9. Department of the Navy /Assistant for Administration (DON/AA) will:

a. Establish reporting guidelines and procedures for personnel within the Secretariat to refer relevant insider threat information directly to the DON ITP.

b. Ensure personnel within the Secretariat are included in and trained in accordance with the DON ITP.

c. Collaborate with the DON Insider Threat Hub to ensure the Secretariat personnel are monitored, responded to, and represented in the same manner as the DON personnel who fall within the confines of this instruction.

d. Provide analysts to DON Insider Threat Hub in order to cover DON Secretariat personnel.

10. Surgeon General of the Navy will:

a. Provide medical and psychological expertise to the DON Insider Threat Hub to advise on clinical issues relevant to the behaviors observed.

b. Provide the DON Insider Threat Hub with access to personal health information, as authorized, in accordance with applicable laws, policies, regulations, and orders.

c. Plan, program, and budget the resources to carry out DON ITP medical and psychological screenings, as required to assist in determining security risks.

d. Provide medical or psychological representatives to DON ITP chartered working groups as required.

11. JAG will:

a. Provide legal advice and review on subject matters listed in this instruction that fall under JAG cognizance.

b. Provide legal support to DON ITP chartered working groups, as appropriate.

12. The Naval IG will:

a. Conduct independent and objective inspections of the DON ITP for compliance, effectiveness, and adherence to higher authority guidance and policy. Ensure access to related records and data is restricted only to insider threat personnel who require the information to perform their authorized functions.

b. Provide IG representative(s) to DON ITP chartered working groups.

13. Director, DON Special Access Program Central Office (SAPCO) will:

a. Integrate with the DON Insider Threat Hub for Special Access Program (SAPs) in accordance with reference (o).

b. Serve as the requirements and resource sponsor for ITP for SAPs, per reference (o).

c. Conduct UAM on DON SAP Networks.

d. Serve as a member of the DON SE EXCOM as described in reference (h).

e. Provide a DON SAPCO representative(s) to DON ITP chartered working groups.

14. The DON SE EXCOM is the senior-level governance body responsible for administration, strategic guidance, and policy authority for the DON Security Enterprise (DON SE). A complete list of responsibilities for the DON SE EXCOM can be found in reference (h). The DON SE EXCOM will incorporate the DON ITP within its purview.

15. Senior Director for Security and Intelligence will:

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

b. Provide oversight for the DON ITP and coordinate with other stakeholders to promulgate policy.

c. Oversee the establishment and operation of DON Insider Threat Hub.

d. Ensure processes are developed and implemented that the DON Insider Threat Hub will use to centrally gather, integrate, analyze, and respond to information indicative of a potential insider threat.

e. Ensure the DON Insider Threat Hub reports to the DITMAC in accordance with the DITMAC Reporting Thresholds detailed in reference (i).

f. Ensure the DON ITP includes, either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on classified networks in order to detect activity indicative of insider threat behavior.

g. Designate a MICP Coordinator for the DON ITP in writing to manage ITP MICP responsibilities under the guidance of the DUSN MICP Coordinator and in accordance with reference (p).

16. CMC and CNO will:

a. Support the establishment of a single DON Insider Threat Hub to gather, integrate, review, assess, and respond to anomalous information derived from AT/FP, CI, CS, civilian and military personnel management, LE, PAR, Security, UAM, and other sources as necessary and appropriate.

b. Establish procedures to implement the use of PAR capabilities, as described in reference (m), at the installation level, including bases, stations, and joint bases; and in other organizations as directed by the Senior Official. Establishment of a PAR capability is not required if a PAR-like capability already exists.

c. In accordance with reference (m), ensure that the developed insider threat capability aligns with and complements PAR capabilities and functional experts in order to identify personnel at risk for potentially violent behaviors.

d. Ensure procedures for access requests by the DON ITP involving particularly sensitive or protected information, such as information held by special access, LE, inspector general, or other investigative sources or programs are utilized and enforced.

e. Utilize procedures established by ASN (M&RA) to access civilian and military personnel management records and other relevant sensitive or protected information for DON employees (see definition of “employee” in enclosure (2)).

f. Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the ITP or one of its stakeholders.

g. Develop guidelines and procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of the matter.

h. Establish, consistent with applicable law, regulation, and policy, reporting guidelines for CI, Security, CS, civilian and military personnel management, and other relevant

organizational components to refer relevant insider threat information directly to the DON Insider Threat Hub.

i. Ensure the DON ITP has timely access, as otherwise permitted, to available U.S. Government intelligence and CI reporting information and analytic products pertaining to adversarial threats.

j. Program and conduct UAM on respective classified networks.

k. Develop an implementation plan and report annually to the DON Insider Threat Senior Official in regards to respective ITP accomplishments, resource requirements, insider threat risks, program impediments or challenges, and recommendations for program improvements. Annual reports will cover the preceding fiscal year and must be submitted to the DON Insider Threat Senior Official by November 1st.

l. Ensure personnel assigned to the DON ITP are trained in the following subject matters, in addition to the CI Awareness and Reporting training conducted by NCIS:

(1) Established procedures for insider threat response actions.

(2) Security fundamentals, to include applicable legal issues.

(3) Applicable law, regulation, and policy regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.

(4) Applicable civil liberties and privacy law, regulation, and policy, including the DON Breach Response Plan.

(5) Investigative referral requirements of references (c) and (j) as well as other policy or statutory requirements that require referrals to an internal entity or external investigative entities. Referral requirements will be the responsibility of NCIS.

m. Ensure that insider threat training requirements include and apply to all personnel employed by, detailed to, or assigned to their respective services. Provide and verify cleared employees under the DON receive training within 30 days of initial employment, entry on duty, or following the granting of access to classified information and annually thereafter in the following topics:

(1) The importance of detecting potential insider threats and reporting suspected activity to insider threat personnel or other designated officials;

(2) Methodologies of adversaries to recruit trusted insiders and collect classified information;

(3) Indicators of insider threat behavior and procedures to report such behavior; and

(4) CI and security reporting requirements, as applicable.

n. Coordinate DON ITP access to required data streams in accordance with applicable law, regulation, and policy.

o. Ensure, when necessary, that all network Service Level Agreements outline the capabilities the network provider will employ to identify suspicious user behavior and how that information must be reported to the DON ITP.

p. Ensure the respective service ITPs comply with the minimum standards described in reference (b) in support of the DON ITP.

q. Serve as a member of the DON SE EXCOM as described in reference (h).

r. Provide appropriate representative(s) to DON ITP chartered working groups upon request.

17. In addition to paragraph 6 of this enclosure, the CNO will:

a. Be responsible for the DON Secretariat ITP, to include PAR, or PAR-like, capabilities.

b. Collaborate with DON/AA for DON Insider Threat Hub matters regarding DON Secretariat personnel.