



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

OPNAVINST 5510.165A
DNS
1 Oct 2015

OPNAV INSTRUCTION 5510.165A

From: Chief of Naval Operations

Subj: NAVY INSIDER THREAT PROGRAM

Ref: (a) E.O. 13587
(b) DoD Directive 5205.16 of 30 September 2014
(c) SECNAVINST 5510.37
(d) DoD Instruction 5240.26 of 4 May 2012
(e) CNO WASHINGTON DC 132027Z Dec 13 (NAVADMIN 319/13)
(f) SECNAVINST 1730.10
(g) OPNAVINST 5450.345

Encl: (1) Navy Insider Threat Program Implementation Plan

1. Purpose

a. To establish the Navy Insider Threat Program (ITP) per reference (a), issue policy, assign responsibilities, and institute the Navy Insider Threat Board of Governance (NITBOG).

b. Changes to this revision include the addition of a Navy ITP implementation plan. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 5510.165.

3. Scope and Applicability. This instruction applies to all U.S. Navy commands and activities. Governance is applicable to all appropriate Navy enterprise antiterrorism/force protection (AT/FP), counterintelligence (CI), human resources (HR), cyber security (cyber), information assurance (IA), law enforcement (LE), security, and other authorities and processes that impact or influence insider threat deterrence, detection, and mitigation capabilities.

4. Background

a. Per reference (a), the President directed that any and all agencies that "operate or access classified computer

networks" establish ITPs consistent with the Insider Threat Task Force established in reference (a), section 6 to ensure responsible and secure sharing and safeguarding of classified material.

b. Reference (b) provides further guidance on Department of Defense (DoD) requirements of ITPs.

c. The Secretary of the Navy (SECNAV) issued reference (c) to guide development of the Department of the Navy (DON) ITP, designating the Deputy Under Secretary of the Navy for Policy (DUSN Policy) as the DON ITP lead.

d. Per reference (d), an insider threat is anyone "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."

5. Policy

a. In addition to overarching DON policy in reference (c), paragraph 5, the Navy will:

(1) Plan, program and implement enhanced technical capabilities to monitor user activity on all Navy networks and systems per national, DoD, and SECNAV policies and directives.

(2) Plan, program and implement enhanced continuous evaluation of all Navy personnel under national, DoD, and SECNAV policies and directives.

(3) Leverage and coordinate AT/FP, CI, HR, cyber, IA, LE, security, and other authorities and processes to improve existing insider threat detection and mitigation efforts.

b. The NITBOG is established to provide oversight and guidance to a Navy federated, uniform, and comprehensive insider threat detection, mitigation, and response strategy, and provide senior leadership recommended actions, prioritization, planning, programming, information sharing, and execution of activities in

support of a comprehensive Navy ITP per applicable laws, policies, regulations, directives, and orders. Specifically, the NITBOG will:

(1) Submit a NITBOG charter for approval to the Chief of Naval Operations (CNO).

(2) Exercise oversight, management, and review overall Navy insider threat plans and programs.

(3) Provide oversight of Navy ITP analytic and response capability and issue governing policy and procedure for its effective implementation.

(4) Receive reports from the Navy ITP annually, or as deemed necessary by the chair.

(5) Ensure privacy rights are safeguarded and associated process protections are routinely reviewed for efficacy.

(6) Meet quarterly or as required by the chair.

(7) Charter a Navy insider threat working group to provide recommendations and assist the NITBOG with oversight management responsibilities and policy implementation.

6. NITBOG Membership. The NITBOG will be chaired by the Director, Navy Staff (DNS). DNS may augment membership, as appropriate.

a. NITBOG Principal Members

(1) Deputy Chief of Naval Operations for Manpower, Personnel, Education, and Training (CNO N1)

(2) Deputy Chief of Naval Operations for Information Dominance (CNO N2/N6)

(3) Deputy Chief of Naval Operations for Operations, Plans, and Policy (CNO N3/N5)

(4) Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO N4)

(5) Deputy Chief of Naval Operations for Integration of Capabilities and Resources (CNO N8)

(6) Commander, U.S. Fleet Cyber Command (COMFLTCYBERCOM) and Commander, U.S. Tenth Fleet (COMTENTHFLT)

(7) Deputy Director, Naval Criminal Investigative Service (NCIS)

b. Advisory Members. The NITBOG chair may invite advisory members to attend meetings and or provide relevant information as necessary. Advisory members include, but are not limited to:

(1) Chief of Navy Reserve (CNO N095)

(2) Navy Chief of Information (CHINFO)

(3) Director, Navy Intelligence Protection and Oversight (OPNAV N2/N6IP)

(4) Surgeon General of the Navy (CNO N093)

(5) Judge Advocate General (JAG) of the Navy

(6) Chief of Chaplains (CNO N097)

(7) Director, Special Programs (OPNAV N89)

c. NITBOG Executive Secretariat. The Deputy Director, Navy Staff (DDNS), or a designated delegate, will serve as executive secretariat of the NITBOG, execute tasking, and oversee chartered NITBOG special working groups including chairing the Navy Insider Threat Working Group. The Navy Insider Threat Working Group will, at a minimum, include representation from the organizations listed in subparagraphs 6c(1) through 6c(7).

(1) CNO N1

(2) OPNAV N2/N6IP

(3) OPNAV Antiterrorism/Force Protection (N314)

(4) OPNAV Shore Readiness (N46)

(5) CNO N8

(6) NCIS Insider Threat Division

(7) Additional Navy Insider Threat Working Group members may be assigned as directed by the NITBOG.

7. Responsibilities

a. DNS, as the designated senior official of the Navy ITP, will:

(1) Execute oversight and management of the Navy ITP.

(2) Direct Navy capability, resource, planning and programming efforts to effectively detect, deter, and mitigate insider threats.

(3) Manage the Navy ITP across all mission areas, programs, activities, processes, and procedures, per reference (a).

(4) Represent Navy ITP as a principal member of the DON ITP Senior Executive Board, per reference (c).

(5) Develop and implement, via the NITBOG, a process for reporting information and or details of incidents indicative of an insider threat to the Navy ITP analytic and response capability.

(6) Carry out appropriate tasks as identified in enclosure (1).

b. JAG will provide advice and counsel to the Navy ITP on legal issues, privacy matters and other areas, as appropriate.

c. During command inspections and area visits, NAVINSGEN inspectors will review Navy ITP implementation as appropriate and, if necessary, report findings in inspection reports.

d. CNO N2/N6, through OPNAV N2/N6IP, will:

(1) Maintain an insider threat to cyber security program office and portfolio as the designated Navy lead for insider threat to cyber-based aspects of the Navy ITP.

(2) Coordinate and manage the CI, IA, cyber, anomaly detection, continuous evaluation, and special security mission areas in support of DNS.

(3) Ensure the development, planning for, programming, effective implementation and maintenance of an automated insider threat analytic and response capability, as directed in references (b), (c), and (e), that has the capability to gather, integrate, review, assess, and appropriately refer anomalous information derived from AT/FP, CI, HR, cyber, IA, LE, security, anomaly detection, continuous evaluation and other sources as necessary and appropriate.

(4) Ensure the Navy ITP has access to appropriate data streams and records to the extent consistent with applicable laws, policies, regulations, and orders.

(5) Ensure personnel assigned to insider threat to cyber security duties, regardless of Service affiliation, receive standardized integrated training as required by references (b) and (c).

(6) Incorporate insider threat cyber-based requirements into planning, programming, and budgeting as applicable to support the Navy ITP.

(7) Conduct periodic evaluation and reviews of the insider threat mission area and cyber capability and capacity seams, gaps, and resource planning. Provide resource and acquisition guidance necessary for ITP wholeness and effectiveness. This includes, but is not limited to, advocating for resourcing for insider threat or other IA programs that would effectively support a Navy holistic ITP.

(8) Ensure Navy ITP analytic and response capability is established and managed per Office of the Chief of Naval Operations (OPNAV) directives.

(9) Receive and implement, as appropriate, recommended changes to Navy insider threat information technology capabilities from OPNAV N2/N6IP.

(10) In coordination with NCIS and appropriate Navy training and education entities, develop and issue a Navy insider threat training plan for Navy ITP personnel, and a Navy insider threat to cyber security awareness training for all Navy personnel to include military, civilians, and contractors.

(11) Carry out appropriate tasks as identified in enclosure (1).

e. CNO N1 will:

(1) Ensure insider threat and information technology privileged user information is included, to the extent appropriate and permissible under applicable law and policy, in personnel accession screenings, documented in personnel records, and included as a covered subject at appropriate education and training venues.

(2) Ensure that Navy ITP personnel receive access to HR data streams and records to the extent appropriate and consistent with applicable laws, policies, regulations, and orders.

(3) Incorporate insider threat requirements into planning, programming, and budgeting as applicable to support Navy ITP.

(4) Carry out appropriate tasks as identified in enclosure (1).

f. CNO N3/N5, through OPNAV N314, will:

(1) Provide continuous review of AT/FP strategies as they relate to insider threat, personnel security, and physical security in support of DNS.

(2) In coordination with CNO N4; CNO N9; Commander, U.S. Fleet Forces Command; Commander, U.S. Pacific Fleet; and Commander, Naval Installations Command, identify AT/FP related

insider threat gaps and requirements. Incorporate insider threat requirements, as appropriate, into the Planning, Programming, Budgeting, and Execution process.

(3) Communicate and coordinate with all Navy ITP analytic and response capabilities per OPNAV policy.

(4) Carry out appropriate tasks as identified in enclosure (1).

g. CNO N4, through OPNAV N46, will:

(1) Provide and direct resource planning, sponsorship and policy guidance for shore-based AT/FP, LE, and physical security, including prevention and initial response to kinetic incidents.

(2) Communicate and coordinate with all Navy ITP analytic and response capabilities per OPNAV policy.

(3) Carry out appropriate tasks as identified in enclosure (1).

h. CNO N8, through OPNAV N89 will:

(1) Serve as central operational authority for Navy special access program (SAP) networks and support, in coordination with the Navy ITP analytic and response capability, compliance with OPNAV policy and insider threat mitigation mission requirements.

(2) Ensure that Navy ITP personnel receive access to appropriate data streams and records to the extent consistent with applicable laws, policies, regulations, and orders, per reference (c).

(3) Set standards for network security, operational performance, compliance, configuration control, accreditation, and certification to mitigate insider threat risk across the Navy's portion of the SAP networks.

(4) Maintain and share situational awareness of the Navy's portion of the SAP environment commensurate with applicable laws, policies, regulations, and orders.

(5) Incorporate insider threat mitigation requirements into Navy SAP resource planning, readiness assessments, and inspection procedures. Direct resource decisions, including manpower, for applicable operations, missions, and functions supporting insider threat mitigation.

(6) Support privileged user polygraph events with NCIS to ensure that appropriate billets and personnel are identified and injected into the random selection events per reference (e).

(7) Carry out appropriate tasks as identified in enclosure (1).

i. CNO N093 will provide medical and psychological expertise to the Navy ITP including, without limitation, advice pertaining to clinical issues relevant to the behaviors observed, and mitigation of potential insider threat activities in coordination and communication with the Navy ITP analytic and response capability and OPNAV policy.

j. CNO N097 will identify types of information received by CNO N097 that may permissibly be provided to DNS and Navy ITP personnel within the parameters of applicable law and policy, to include references (e) and (f), in coordination with the Navy ITP analytic and response capability, and OPNAV policy.

k. NCIS, as DON executive agent for CI and LE, will:

(1) Provide CI and insider threat awareness and reporting training.

(2) Receive CI and LE referrals for analysis and appropriate CI and LE response, to include status reporting to DON ITP and referral originator, as appropriate, consistent with applicable law and policy, including any disclosure restrictions related to ongoing investigations.

(3) Support the Navy's Random Polygraph Program for privileged users, and consistent with legal and policy disclosure restrictions, provide statistics from polygraph examinations to the NITBOG, per reference (e).

(4) Plan, program, and budget the resources necessary to carry out CI and LE activities in support of the Navy ITP.

(5) Carry out appropriate tasks as identified in enclosure (1).

1. COMFLTCYBERCOM and COMTENTHFLT will:

(1) Serve as central operational authority commensurate with missions delegated per reference (g), and support the insider threat mitigation mission requirements in coordination with the Navy ITP analytic and response capability, in compliance with OPNAV policy for Navy networks.

(2) Ensure that Navy ITP personnel receive access to appropriate data streams and records to the extent consistent with applicable laws, policies, regulations, and orders and reference (c).

(3) Set standards for network security, operational performance, compliance, configuration control, and certification and accreditation to mitigate insider threat risk across the Navy's portion of the DoD information networks.

(4) Ensure coordination and integration of Navy Cyber Defense Operations Command with the Navy ITP analytic and response capability per NITBOG directives.

(5) Incorporate insider threat mitigation requirements into Navy cyber resource planning, readiness assessments, and inspection procedures. Direct resource decisions for applicable COMFLTCYBERCOM and COMTENTHFLT operations, missions, and functions supporting insider threat mitigation.

(6) Maintain oversight of privileged user polygraph requirements to ensure appropriate billets and personnel are included in the continuous or enhanced continuous evaluation program based on their level or depth of access, per reference (e).

(7) Carry out appropriate tasks as identified in enclosure (1).

m. Commander, Office of Naval Intelligence will:

(1) Serve as central operational authority for Navy sensitive compartmented information (SCI) networks and support, in coordination with the Navy ITP analytic and response capability, in compliance with OPNAV policy and insider threat mitigation mission requirements.

(2) Ensure that Navy ITP personnel receive access to appropriate data streams and records to the extent consistent with applicable laws, policies, regulations, orders and reference (c).

(3) Set standards for network security, operational performance, compliance, configuration control, and certification and accreditation to mitigate insider threat risk across the Navy's portion of the SCI networks.

(4) Maintain and share situational awareness of the Navy's portion of the SCI environment commensurate with applicable laws, policies, regulations, and orders.

(5) Incorporate insider threat mitigation requirements into Navy intelligence resource planning, readiness assessments, and inspection procedures. Direct resource decisions, including manpower, for applicable operations, missions, and functions supporting insider threat mitigation.

(6) Support privileged user polygraph events with NCIS to ensure that billets and personnel are identified and injected into the random selection events. See also reference (e).

(7) Carry out appropriate tasks as identified in enclosure (1).

n. Echelon 2 commanders will:

(1) Develop processes to ensure subordinate Navy ITP policies comply with DoD, DON, Navy, and national ITP policies, including, but not limited to, those pertaining to AT/FP, CI, HR, cyber, IA, LE, and personnel security.

(2) Develop procedures for reporting insider threats (actual and potential) through the chain of command to Navy ITP analytic and response centers.

(3) Maintain oversight of privileged user polygraph requirements to ensure appropriate billets and personnel are included in the continuous or enhanced continuous evaluation program based on their level or depth of access. See also reference (e).

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

9. Information Collection Requirements

a. Reporting requirements contained in subparagraphs 5b(4) and 5b(7), and enclosure (1), subparagraph 1a(1), of this instruction are exempt from reports control per SECNAV Manual 5214.1 of December 2005, part IV, subparagraph 7k.

b. Reporting requirements contained in subparagraphs 6a(5), 6j(2), and 6n(2) of this instruction are exempt from reports control per SECNAV Manual 5214.1 of December 2005, part IV, subparagraph 7n.



R. R. BRAUN
Performing the duties of the
Director, Navy Staff

Distribution:

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

NAVY INSIDER THREAT PROGRAM IMPLEMENTATION PLAN

1. The designated senior ITP official will be the office of primary responsibility (OPR) for the tasks and action items outlined in subparagraphs 1a through 1c.

a. Task. Submit annual report on the status of the Navy ITP to CNO.

(1) Action Item. Oversee the preparation of an annual report, for delivery to the CNO, which provides an update on the completion of requirements found in this implementation plan, the National Insider Threat Task Force minimum standards, and DoD and DON ITP policies, resources allocated, insider threat risks identified, recommendations, and goals for program improvement, and which identifies major impediments or challenges to the Navy ITP.

(2) Implementation Timeline. Reports will be delivered to CNO no later than the end of each fiscal year (FY).

b. Task. Facilitate oversight reviews of the Navy's ITP to ensure compliance with policy guidance.

(1) Action Item. As needed, identify, direct, and support Navy subordinate ITP OPRs to assess the status and progress of insider threat program(s) and report the results to appropriate superior organizations. This will include, but not be limited to, requirements to conduct self-assessments and report on their results; program accomplishments; resources allocated; and risks to and goals for the ITP.

(2) Implementation Timeline. Not applicable.

c. Task. As chair of the NITBOG, lead the development of procedures for a centralized system of taking and documenting response actions to insider threat concerns.

(1) Action Item. These procedures will include, but are not limited to, actions by both the Navy insider threat hub personnel (see task in subparagraph 3f) and Navy commands when responding to user activity monitoring and continuous evaluation derived information (see tasks in subparagraphs 3b and 3d). Development of these processes and procedures must be

coordinated with appropriate legal review to ensure that inquiries are conducted within proper limits, that the individual's privacy and civil liberties are protected, that whistleblower protections are enforced, and that the inquiry does not taint evidence or jeopardize a possible investigation or prosecution by a law enforcement agency.

(2) Implementation Timeline. Implementation will be an ongoing process but, at a minimum, must keep pace with the development of the Navy insider threat hub, user activity monitoring, and continuous evaluation programs.

2. CNO (N1) will be the OPR to ensure availability of insider threat awareness training for all Navy personnel.

a. Action Item. In coordination with NCIS and CNO N2/N6, establish access to annual insider threat awareness training for all Navy personnel as well as access to initial and annual training for personnel granted access to classified information. NCIS will develop the training with support from DON per reference (c).

b. Implementation Timeline. Task to be completed by fourth quarter of FY 2015.

3. CNO N2/N6 will be the OPR for the tasks and action items outlined in subparagraphs 3a through 3f.

a. Task. In coordination with COMFLTCYBERCOM and COMTENTHFLT, assess the number of privileged users against requirements with a goal of reducing the total number to the minimum extent practical.

(1) Action Item. Privileged users typically range from those that have slightly elevated privileges to those that have a great deal of access to data and systems in information technology environments and, therefore, could pose a higher risk of insider threat. As such, CNO N2/N6 will lead an effort to identify fleet-wide ways to balance two-party integrity, the principle of least privilege, and the reduction of Navy privileged users.

(2) Implementation Timeline. Annual.

b. Task. Coordinate with appropriate DoD and DON offices and commands to ensure the development of an effective enterprise-wide enhanced continuous evaluation program for all Navy personnel.

(1) Action Items

(a) Integrate lessons learned from the DoD continuous evaluation program into the implementation of a Navy continuous evaluation program.

(b) Develop and coordinate a process for sharing information obtained by continuous evaluation methods with appropriate commands and security personnel.

(c) Disseminate guidance to all commands on requirements and processes for receiving and responding to notifications resulting from the command evaluation process.

(2) Implementation Timeline. To be determined based upon DoD and DON actions to implement a continuous evaluation program.

c. Task. Establish a formalized random polygraph program for the Navy.

(1) Action Item. In coordination with the Director, NCIS, implement a random polygraph program that includes Navy privileged users and other high-risk personnel, as deemed appropriate, to submit to random polygraph exams as directed annually. A privileged user is defined as an individual who has access to system controls, monitoring, or administration functions.

(2) Implementation Timeline. Task to be completed by fourth quarter of FY 2016.

d. Task. Implement user activity monitoring on the Joint Worldwide Intelligence Communications System (JWICS) to include the capability to analyze results.

(1) Action Items

(a) Present to the NITBOG a proposed user activity monitoring implementation timeline for JWICS.

(b) Outline processes to ensure that user activity monitoring-derived data is made available to the Navy insider threat central analytic hub (see subparagraph 3f) for processing and analysis.

(2) Implementation Timeline. Details on implementation of a user activity monitoring are classified.

e. Task. Implement user activity monitoring on the Navy Secret Internet Protocol Router Network (SIPRNET) to include the capability to analyze results.

(1) Action Items

(a) Present NITBOG with resource, material, and manpower requirements to meet this requirement.

(b) Outline processes to ensure that user activity monitoring-derived data is made available to the Navy insider threat central analytic hub (see paragraph 3f) for processing and analysis.

(2) Implementation Timeline. To be determined by the NITBOG following further requirements research led by CNO N2/N6. Implementation of user activity monitoring on SIPRNET will require coordination with and support from DoD and DON level officials.

f. Task. Establish and provide oversight to a Navy centralized insider threat hub to execute three primary functions: gather and integrate information from various sources; analyze that information to identify indications of possible malicious insider activity; and ensure that Navy responds appropriately to all insider threat indicators.

(1) Action Items

(a) Present NITBOG with resource, material, and manpower requirements to establish and operate an analysis hub.

(b) Define "insider threat personnel" as it applies to the Navy. This would be the subset of personnel who require additional specialized insider threat training due to performance of functions and or duties within an ITP, or assigned to an activity that directly supports an insider threat mission.

(c) As the hub is established, develop guidelines and procedures to ensure that records generated in support of the ITP are managed and preserved per guidelines set forth by the DON, Navy and the National Archives and Records Administration.

(d) Ensure insider threat analysts and or managerial personnel within the hub have regular, timely, and, if possible, electronic access to CI, security, IA, HR, and other data as required to support the real-time (or near real-time) identification, analysis, and resolution of insider threat matters.

(2) Implementation Timeline. Hub creation and ultimate connection to the DoD Insider Threat Management and Analysis Center (DITMAC) will be an iterative process driven by many factors, primarily DITMAC development and generation of service requirements. As such, achievement of the Navy's insider threat hub full operating capability is difficult to estimate. Navy, however, will achieve initial operating capability by the end of the fourth quarter FY 2016.

4. CNO N4 will be the OPR to accelerate implementation of the Identity Management Enterprise Services Architecture (IMESA) to enable components to share access control information.

a. Action Item. Determine a resource requirement and deployment plan to conduct operational testing and rollout of IMESA to Navy installations.

b. Implementation Timeline. All Navy installations will have IMESA by the end of the first quarter of FY 2018.

5. CNO N8 will be the OPR for the tasks and action items outlined in subparagraphs 5a and 5b.

a. Task. Provide ITP resource recommendations and requirements to CNO.

(1) Action Item. Determine the additional funding needed to fulfill the requirements detailed within this implementation plan and for any additional requirements as determined by the NITBOG.

(2) Implementation Timeline. Annual requirement.

b. Task. Ensure ITP implementation for SAP, and supporting infrastructure.

(1) Action Item. Direct OPNAV N89 to provide resources and develop implementation plans to meet ITP requirements for SAP, as applicable.

(2) Implementation Timeline. In parallel with Navy ITP initiatives and timelines, pending funding and other factors including SAP enhanced security requirements.