DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

BUMEDINST 5510.9C
BUMED-N45
8 Jul 2024

BUMED INSTRUCTION 5510.9C

From: Chief, Bureau of Medicine and Surgery

Subj: BUREAU OF MEDICINE AND SURGERY INSIDER THREAT PROGRAM

Ref: (a) SECNAVINST 5211.5F
(b) DoD Directive 5205.16 of 30 September 2014
(c) E. O. 13587
(d) SECNAVINST 5510.37A
(e) OPNAVINST 5510.165A
(f) OPNAVINST F3300.53D
(g) BUMEDINST 3300.1B
(h) BUMEDINST 5510.11
(i) SECNAVINST 5510.30C
(j) DoD Instruction O-2000.16 of 17 November 2016
(k) CNO WASHINGTON DC 281639Z Jul 23 (NAVADMIN 170/23)
(l) OPNAVINST F3100.6
(m)DoD Instruction 5400.11 of 29 January 2019
(n) SECNAVINST 5500.35

Encl: (1) Definitions and Acronyms
(2) Forces Protection Executive Board Membership List
(3) Insider Threat Information Flow Chart

1. Purpose. To establish the Bureau of Medicine and Surgery (BUMED) Insider Threat Program (InTP) per references (a) through (m), publish policy, assign responsibilities, reporting criteria, and reporting procedures, and institute the Navy Medicine (NAVMED) insider threat working groups. This instruction is a complete revision and must be reviewed in its entirety.

2. Cancellation. BUMEDINST 5510.9B.

3. Scope and Applicability. This instruction applies to all budget submitting office (BSO) 18 commands, BUMED Headquarters, and is applicable to all appropriate BUMED departments, force protection (FP), counterintelligence, cybersecurity, security, human resources, public affairs, legal, and other authorities, and processes that impact or influence insider threat deterrence, detection, and mitigation capabilities.

4. Background

a. Per references (a) through (e), and (k), all BSO-18 commands must establish an InTP to deter, detect, and mitigate insider threats. Unauthorized disclosures of classified information have caused significant damage to national security. Violent kinetic acts have resulted in loss of life and damage to operational resources. References (a) and (d) defines the Deputy Undersecretary of the Navy for Policy as the Department of the Navy (DON) Insider Threat (InT) lead.

b. Reference (b) provides further guidance on Department of Defense (DoD) and DON InTPs.

c. Reference (d) defines an insider threat as a person or persons who:

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

(2) Wittingly, or unwittingly, commits:

(a) 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

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

5. Policy. BSO-18 commands must establish an integrated set of policies, programs, and procedures to detect, deter, and mitigate insider threats before damage is done to national security or to military personnel, resources, and capabilities. These policies must leverage existing Federal laws, statutes, authorities, policies, programs, systems, architecture, and resources to counter the threat of those insiders who may use their authorized access to compromise classified information. Per reference (m), these policies must employ risk management principles, be tailored to meet the distinct needs for mission, and systems of individual agencies, and complies with all controlling law, regulation, and policy including those regarding whistleblower, civil liberties, cybersecurity, and privacy protection. The InTP is the responsibility of the commander, commanding officer (CO), and officer in charge (OIC) to ensure all reportable information is reported to the proper entities. Failure to share this information could result in the unwarranted acceptance of additional risk by the command.

6. Responsibilities

a. Deputy Director, Maritime Headquarters (BUMED-N03B) and Director, Mission Assurance (BUMED-N45) must:

(1) Provide oversight and guidance to all BSO-18 commands.

(2) Provide recommendations, prioritizations, planning, programming, information sharing, and policy for BSO-18 commands.

(3) Ensure a Force Protection Executive Board (FPEB) is established, which incorporates InT within its charter, and meets at a minimum semi-annually to review and update InTP guidance, policy, and standards. FPEB membership is outlined within enclosure (2).

(4) BUMED-N45 will assess the echelon 3 commands InTP annually, ensuring their program is compliant and oversight conducted. Echelon 3 commands will be responsible for oversight of echelon 4 commands and will assess these commands every two years at a minimum. Echelon 4 commands will provide oversight and assess their echelon 5 commands every 2 years at a minimum. This assessment may be virtual if funds do not permit travel.

(5) Disseminate any pertinent insider threat information and training to the echelon 3 InT managers.

(6) Per reference (k), subparagraph 3d identifies sources of training for the command staff. Ensure all BSO-18 military, civilian, and contractor staff, complete the InT awareness training, DON-CIATR-1.0-NCIS Counterintelligence and Insider Threat Awareness and Reporting Training available in the Total Workforce Management Services (TWMS) at https://twms.dc3n,navy.mil/logon.asp. Training must be completed within 30 days of reporting onboard, and annually thereafter. The command InTP manager must maintain awareness of the completion percentages of the command, which is 100 percent completion for the command.

(7) Per references (b), (d), (e), and (n), ensure corresponding programs are current and executable. At a minimum, the programs included in BSO-18's InTp:

(a) FP Program.

(b) Personnel Security Program.

(c) Physical Security Program.

b. Director, Manpower and Personnel (BUMED-N1) must ensure insider threat information is included in all of the BSO-18 personnel accession screenings and personnel records.

c. Director, Education and Training (BUMED-N7) will ascertain the appropriate education and training venues.

d. Director, Communication and Information Systems (BUMED-N6) will comply with references (a) through (m) and ensure all requirements for higher headquarters cyber and information systems are adhered to, and that annual user training is completed and documented. BUMED-N6 must also ensure all information systems possess an authorization to operate and appropriate cybersecurity controls (e.g., risk management framework) to mitigate insider threat.

e. Director, Logistics, Supply, and Support (BUMED-N4) must coordinate with the Staff Judge Advocate (BUMED-N01J) to ensure input to, and oversight of, the Navy InTP in protecting and safeguarding all legal, civil, and privacy rights of BSO-18 personnel, per references (b) through (d).

f. Director, Medical Inspector General (BUMED-N00IG) will incorporate InT inspection line items into the existing InT inspection tool for inspection of this program.

g. Echelon 3, 4, and 5 commanders, COs, officers in charge, and BUMED Headquarters and their detachments must meet the requirements of this instruction and:

(1) Designate, in writing, an InTP manager, who must obtain and maintain a favorably adjudicated Tier 3 background investigation.

(2) Ensure insider threat training for newly reporting staff incorporates command-specific policy and procedures ensuring staff members are aware of command reporting procedures.

(3) Identify, document, and prioritize organizational sensitive assets.

(4) Reporting of potential InT activities must be accomplished via the command InTP manager or may be reported directly to the InT Hub by any member of the command. The InT Hub is an analytic resource to commands for all insider threat matters to include supporting risk management decisions and facilitate appropriate response actions to reduce this risk across the Navy. Reporting information to the Hub is not punitive in nature, but a resource with various data base resources. The information held by the Hub may or may not be known to the command but provides a holistic picture of the member allowing the command greater knowledge to move forward.

(5) The reporting criteria is listed in reference (k), subparagraph 3e(1). Additionally, per reference (l), include the plain language address directory NAVY INSIDER THREAT HUB ELEMENT WASHINGTON DC, will be added on all Operation Reports and Situation Reports that meets criteria below and in reference (k) for mandatory reporting to the InT Hub.

(6) Reference (k), subparagraph 3e(1), contains a list of potential risk indicators (PRI). PRIs are actions individuals take which could become a risk of becoming an insider threat, and those actions could ultimately cause significant harm. Warning signs are often exhibited, and staff members should be cognizant of these actions and report these to supervisor or other designated personnel. PRIs include a wide range of individual predispositions, stressors,

choices, actions, and behaviors. Some indicators suggest increased vulnerability to insider threat; others may be signs of an imminent or serious threat. These PRIs must be used to determine if the commands action should be reported to the DON InT Hub. If PRIs are identified early, many risks may be mitigated before harm to the command occurs.

(7) Enclosure (2) is an example of the information flow within the command. It should be noted, the activity security manager has similar reporting requirements as the InTP manager and the two program managers must work in concert of each other.

(8) After reporting an incident to the DON InT Hub, the InT Hub will send the command a Navy insider threat risk analysis (ITRA) memorandum. Within 30 days of receipt of ITRA memorandum, the command must report back to the Hub all actions taken and provide the mitigating actions taken.

(9) Commanders at all levels will ensure any behavior associated with the PRIs is passed to the InT manager, activity security manager, legal office, and human resources office personnel to make the proper notifications and take the required actions. Information flow between these separate and distinct codes must be interactive and flow in both directions. This will assist in having a fully executable and efficient InTP. This information must be held in the strictest confidence and only shared with those with a need-to-know.

(10) Commands must establish their own clear reporting guidelines and procedures. Ensure staff are trained and understand the reporting process.

(11) Commands are encouraged to include the below entities when developing the notification matrix. These entities either have reporting requirements separate of the InTP or have the subject matter expertise to assist in bringing these issues to a successful resolution.

(a) Activity security manager.

(b) Command InT manager.

(c) Human resources office.

(d) Supervisor, division officer, leading chief petty officer.

(e) Command staff judge advocate or legal officer.

(f) Naval Criminal Investigative Service.

(12) Develop a means of follow-up to the reporting party.

(13) Implement a system to collect and correlate data while always protecting the privacy of those reporting and reported.

(14) Develop and establish procedures for recommending an appropriate response based on the recommendations and information received from the DON InT Hub.

(15) Develop a local InT instruction which delineates specific responsibilities to the command as well as subordinate commands.

(16) Ensure all InT information and or training is provided to command staff and subordinate commands. Leverage all InT information and, in coordination with command security managers, conduct InT training in conjunction with annual counterintelligence awareness and reporting training.

(17) Establish a local InT working group. Incorporation of the InT into an existing force protection board or antiterrorism working group, that meets at a minimum semi-annually, is acceptable, per references (f) through (i). Ad hoc meetings are acceptable and encouraged to determine a command response.

(18) Echelon 3 commanders must ensure their echelon security managers comply with this instruction and references (a) through (m).

h. Per reference (m), the command must consider all the fair information practices (e.g., notice to the workforce), and the necessary privacy and security safeguards, to include role-based access to the data collected, and oversight of the program personnel and system administrators. However, this information must be shared with, at a minimum, the antiterrorism officer, InT manager, and the command security manager.

(1) The information should be reviewed for credibility and accuracy prior to command administrative or disciplinary action. The InTP should ensure that any inaccuracies it has found are remedied and corrections are passed along to recipients of the erroneous data.

(2) Information may only be used for the purpose reported; it may not have any secondary uses unrelated to the insider threat activity, unless authorized by law or regulation. If further administrative or punitive action is considered, commands should consult with the cognizant staff judge advocate, counsel, or legal officer.

(3) When making a report of a possible insider threat, it is vital that all employees are aware of the reporting process and the confidentiality of the report. Employees and other covered persons should be provided the address or link to the applicable privacy impact assessments, system of records notices, and departmental directives, instructions, and standard operating procedures.

(4) InT managers must work closely with the command's legal department to ensure all privacy and confidentiality is afforded to all parties.

(5) Echelon 4 and 5 commands, at the discretion of the CO, may contact the DON InT Hub. Notification to the echelon 3 InTP manager must be made by email or phone as soon as practical after reporting to the InT Hub. The link is provided in subparagraph 6h(7) of this instruction.

(6) The DON InT Hub receives information related to potential insider threat concerns, determines insider threat nexus, conducts analysis of potential risks to the DON, and provides insider threat assessments/mitigation recommendations as appropriate.

(7) All DON personnel may report potential insider threat activity or concerns directly to the DON Int Hub by submitting a report through the DON InT Hub portal at https://www.secnav.navy.mil/itp, e-mail, insiderthreat.fct@navy.mil, or phone (703) 695-7700.

(8) It is the responsibility of all hands to report any suspicious acts described in this instruction, any workplace violence, or other action or act conducted by a co-worker which could cause damage to national security, or pose a danger to self, or staff.

7. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Directorate for Administration, Logistics, and Operations, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/ DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/ AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the DON Directorate for Administration, Logistics, and Operations, Directives and Records Management Division program office.

8. Review and Effective Date. Per OPNAVINST 5215.17A, BUMED-N4 will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

9. Information Management Control. The reports required in subparagraph 6f are exempt from reports control per SECNAV Manual 5214.1 of December 2005, part IV, subparagraph 7c.

D. K. VIA

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site, https://www.med.navy.mil/Directives/

DEFINITIONS AND ACRONYMS

1. Insider Threat. Is a person or persons 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.

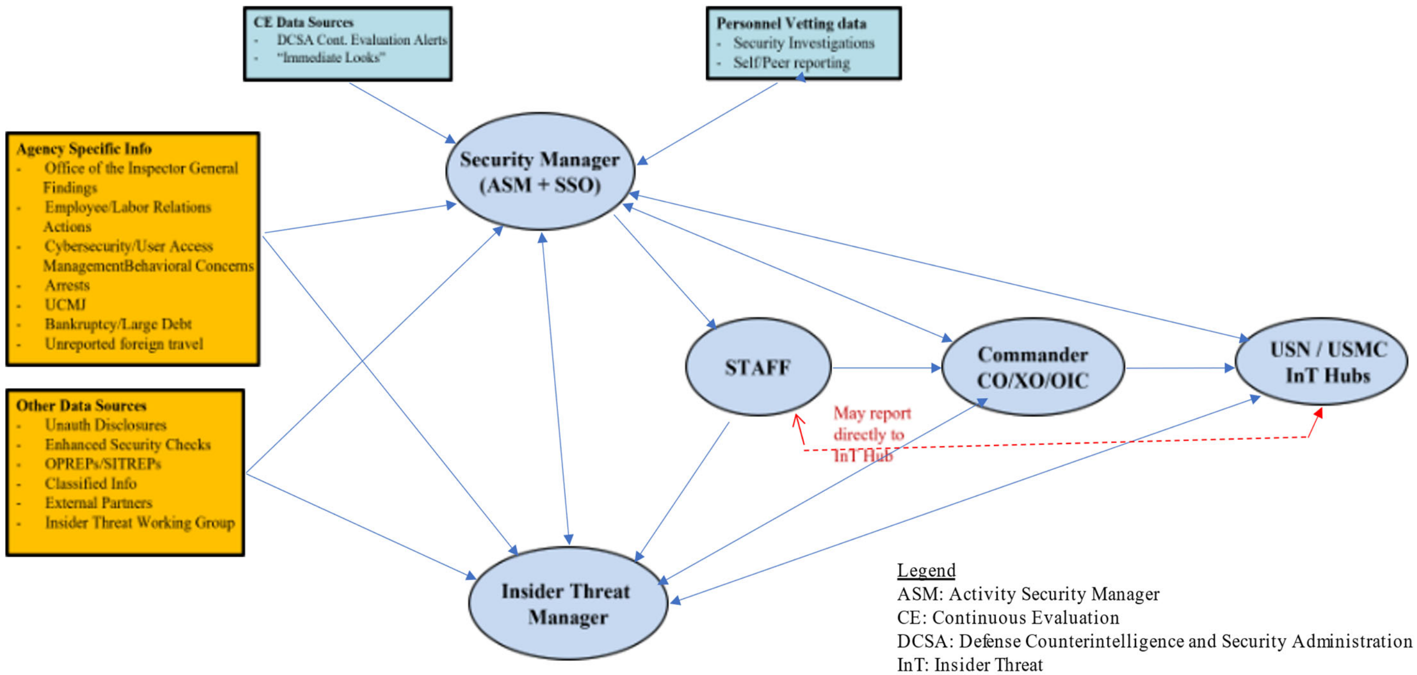
2. Insider Threat Hub. An insider threat analytic and response activity which gathers, integrates, reviews, assesses, and responds to information derived from counterintelligence, security, cybersecurity, human resources, law enforcement, inspector general, and other sources as necessary and appropriate.

3. PRI. Individuals at risk of becoming insider threats, and those who ultimately cause significant harm, often exhibit warning signs, or indicators. PRI include a wide range of individual predispositions, stressors, choices, actions, and behaviors. Some indicators suggest increased vulnerability to insider threat; others may be signs of an imminent and serious threat.

FORCE PROTECTION EXECUTIVE BOARD MEMBERSHIP

Team Member	Role/Responsibility
Director, Maritime Headquarters	Board Chair
Deputy Director, Maritime Headquarters	Board Co-Chair
Core Members:	
Director, Fleet Support and Logistics (BUMED-N4)	Coordinator
BUMED, AT/FP Program Director (BUMED-N452)	Coordinator
Staff Judge Advocate	Member
Director, Manpower and Personnel (BUMED-N1)	Member
Civilian Personnel Policy (BUMED-N11)	Member
Director, Research and Development (BUMED-N2)	Member
Director, Operations (BUMED-N3)	Member
Emergency Management Program Manager (BUMED-N453)	Member
Senior Public Health Emergency Officer (BUMED-N44)	Member
Personnel Security Program Manager, BUMED (BUMED-N451)	Member
Director, Plans (BUMED-N5)	Member
Director, Information Management and Technology (BUMED-N6)	Member
Director, Training and Education (BUMED-N7)	Member
Director, Resource Management (BUMED-N8)	Member
Director, Capability Requirements (BUMED-N9)	Member
Antiterrorism Officer, Naval Medical Forces Atlantic	Member
Antiterrorism Officer, Naval Medical Forces Pacific	Member
Antiterrorism Officer, Naval Medicine Support Command	Member
Navy InT Hub Senior Analyst	Ad Hoc member
Naval Criminal Investigative Service Agent (Counterterrorism)	Ad Hoc member, if required

INSIDER THREAT INFORMATION FLOW CHART


CE Data Sources
- DCSA Cont. Evaluation Alerts
- "Immediate Looks"
Personnel Vetting data
- Security Investigations
- Self/Peer reporting
Agency Specific Info
- Office of the Inspector General Findings
- Employee/Labor Relations Actions
- Cybersecurity/User Access ManagementBehavioral Concerns
- Arrests
- UCMJ
- Bankruptcy/Large Debt
- Unreported foreign travel
Other Data Sources
- Unauth Disclosures
- Enhanced Security Checks
- OPREPs/SITREPs
- Classified Info
- External Partners
- Insider Threat Working Group
Security Manager (ASM + SSO)
STAFF
Commander CO/XO/OIC
USN / USMC InT Hubs
May report directly to InT Hub
Insider Threat Manager

Legend
ASM: Activity Security Manager
CE: Continuous Evaluation
DCSA: Defense Counterintelligence and Security Administration
InT: Insider Threat
OPREP: Operations Report
PRI: Potential Risk Indicators
SITREP: Situation Report
SSO: Special Security Officer
UCMJ: Uniform Code of Military Justice