



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

BUMEDINST 5510.9C CH-1  
BUMED-N45  
18 Mar 2026

BUMED INSTRUCTION 5510.9C CHANGE TRANSMITTAL 1

From: Chief, Bureau of Medicine and Surgery

Subj: BUREAU OF MEDICINE AND SURGERY INSIDER THREAT PROGRAM

Encl: (1) Revised page 1  
(2) Revised page 4  
(3) Revised page 5

1. Purpose. To transmit new pages 1, 4 and 5 which provide clarification for all Bureau of Medicine and Surgery commands and activities on the requirement for guidelines and procedures for documenting each insider threat incident reported to the Department of the Navy Insider Threat Hub.

2. Action

a. Remove page 1 of the basic instruction and replace with enclosure (1) of this change transmittal.

b. Remove page 4 of the basic instruction and replace with enclosure (2) of this change transmittal.

c. Remove page 5 of the basic instruction and replace with enclosure (3) of this change transmittal.

3. Records Management

a. Records created as a result of this change transmittal, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Assistant for Administration, 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>.

BUMEDINST 5510.9C CH-1  
18 Mar 2026

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 OPNAV Records Management Program (DNS-16).



R. FREEDMAN  
Acting

Releasability and distribution:

This change transmittal is cleared for public release and is available electronically only via the Navy Medicine Web site, <https://www.med.navy.mil/Directives/>



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

CH-1 of 18 Mar 2026

BUMEDINST 5510.9C

BUMED-N45

8 Jul 2024

BUMED INSTRUCTION 5510.9C

From: Chief, Bureau of Medicine and Surgery

Subj: 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 5510.165B  
(f) OPNAVINST F3300.53D  
(g) BUMEDINST F3300.1C  
(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 F3100.6K  
(m) DoD Instruction 5400.11 of 29 January 2019  
(n) SECNAVINST 5500.35

Encl: (1) Definitions and Acronyms  
(2) Force 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 (n), 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 should be reviewed in its entirety.

2. Cancellation. BUMEDINST 5510.9B.

3. Scope and Applicability. This instruction applies to all Budget Submitting Office (BSO) 18 activities and is applicable to all 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.

information systems are adhered to, and 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 Office of the General Counsel (BUMED-N01L) or 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-N01IG) 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), subparagraphs 3e and 3e(1). Additionally, per reference (l), the plain language address directory, NAVY INSIDER THREAT HUB ELEMENT WASHINGTON DC, will be added on all operation reports and situation reports per reference (k) for mandatory reporting to the InT Hub.

(6) Reference (e), enclosure (2), 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. These PRIs must be used to determine if the command's 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 guidelines and procedures for documenting each InT alert reported to the DON InT Hub, as well as the mitigating actions taken, and ensure the timely resolution of the matter.

(11) Commands are encouraged to include the entities listed in subparagraphs 6g(11)(a) through 6g(11)(f) 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, Office of General Counsel 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.