



**DEPARTMENT OF THE NAVY**  
NAVAL LEGAL SERVICE COMMAND  
1322 PATTERSON AVENUE SE, SUITE 3000  
WASHINGTON NAVY YARD DC 20374-5066

CNLSCINST 5510.1  
N1  
16 Jan 2025

COMNAVLEGSVCCOM INSTRUCTION 5510.1

From: Commander, Naval Legal Service Command

Subj: INSIDER THREAT PROGRAM

Ref: (a) OPNAVINST 5510.165B  
(b) CNO WASHINGTON DC 281639Z Jul 23 (NAVADMIN 170/23)  
(c) SECNAVINST 5510.37A  
(d) DODD 5205.16  
(e) SECNAVINST 5510.30C  
(f) JAGINST 5400.2  
(g) Security Servicing Agreement between the Judge Advocate General,  
Commander, Naval Legal Service Command and Lead Special Trial Counsel of  
November 2024  
(h) OPNAVINST F3100.6K

Encl: (1) Definitions

1. Purpose. To establish Naval Legal Service Command (NLSC) Insider Threat (InT) policy, disseminate reporting procedures, and assign responsibilities per references (a) through (d) to prevent, deter, detect, and mitigate the threat insiders may pose to NLSC facilities, personnel, missions, or resources.

2. Scope and Applicability.

a. This instruction applies to all military, civilian, and contractor personnel assigned, detailed to, visiting, or occupying space at NLSC headquarters (HQ), Victim's Legal Counsel Program (VLCP), Trial Counsel Assistance Program (TCAP), Defense Counsel Assistance Program (DCAP), and NLSC echelon 3 commands, detachments, and branch offices.

b. This instruction does not supersede requirements to refer information on criminal or counterintelligence (CI) allegations, 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 Department of the Navy (DON) to Naval Criminal Investigative Service (NCIS) as expeditiously as possible. Referral to NCIS will not be delayed for any reason, to include concurrent adjudicative, investigative and other administrative actions, for matters that fall within the jurisdiction of NCIS per reference (e).

3. Background. As a result of unauthorized disclosure of classified information that damaged national security and the implementation of the Trusted Workforce 2.0, the President directed the establishment of InT programs.

4. Guiding Principles.

a. The NLSC enterprise is subject to insider threats and will take actions to mitigate or eliminate those threats.

b. The NLSC enterprise will continually identify and assess internal and external threats to the organization and its personnel, and institute programs to defeat threats within applicable guidance and regulation.

c. The NLSC InT program will support implementation of the Trusted Workforce when reviewing cleared positions for continuous evaluation and continuous vetting.

5. Policy. The protection of NLSC personnel and the protection of sensitive or classified material is directly related to the effectiveness of a proactive security program, to include a program that is implemented to deter, detect, and defend against insider threat. The objective of the NLSC InT program is to:

a. Ensure continuous evaluation of all NLSC personnel under the DoD and DON policy is active and items reported as necessary.

b. Ensure coordination with antiterrorism, force protection, counterintelligence, human resources, cyber security, information assurance, law enforcement, security, and other authorities to meet InT program reporting requirements.

c. Provide NLSC personnel awareness training on InT and InT reporting responsibilities.

d. Complete self-assessments or self-inspections as directed by higher authority, and report when required.

e. Prevent espionage or unauthorized disclosure of sensitive or classified information.

f. Prevent violent acts against NLSC personnel in the workplace.

g. Deter cleared employees from becoming insider threats.

h. Detect employees who pose a risk to sensitive or classified information systems and information.

i. Mitigate, to the extent practicable, the risks to the security of NLSC facilities, personnel, and information through administrative, investigative, or other responses.

6. Roles and Responsibilities.

a. The NLSC InT Representative will:

(1) Be designated in writing by the Commander, NLSC. In accordance with references (f) and (g) and with the consent of the Assistant Judge Advocate General of the Navy (Operations and Management), a member of the Office of the Judge Advocate General Security Office will be designated as the NLSC InT Representative.

(2) Maintain the InT program as prescribed by references (a) through (d) and coordinate with the Navy InT Hub as needed.

(3) Ensure all cleared military, civilian, and contractor personnel at NLSC HQ, VLCP, TCAP, and DCAP complete InT awareness training as required by reference (a) (Navy eLearning: DON-CIAR-1.0-NCIS Counterintelligence and Insider Threat Awareness and Reporting; Waypoints: 00-DON-NCIS Counterintelligence and Insider Threat Awareness and Reporting Training). Training must be completed within 30 days of initial employment, entry-on-duty or following the granting of access to classified information and annually thereafter. Maintain records of training completion.

(4) Develop guidelines and procedures for documenting each NLSC enterprise InT alert reported to the Navy Hub and response action(s) taken and ensure the timely resolution of the matter.

(5) Report potential NLSC HQ InT concerns or incidents, per enclosure (2) of reference (a), directly to the Navy InT Hub. Use OPNAV 5510/423 (Navy Insider Threat Report) to submit InT reports. Upon receipt of a response from the Navy InT Hub, report all mitigating actions taken within 30 days.

(6) Submit an OPREP-3 message as required by reference (h). If an OPREP-3 message is required, ensure the Navy Hub is notified via separate correspondence of the reportable information contained in enclosure (2) of reference (a), and contact the Navy Hub to provide PII information regarding the subject(s) involved.

(7) Review security violations in the NLSC enterprise and track the number of violations annually to help identify common themes, trends, and corrective actions.

(8) Ensure NLSC HQ, VLCP, TCAP, and DCAP personnel are aware of the reporting criteria and how to report information to the NLSC InT Representative.

(9) Provide advice and support to the echelon 3 command InT Representatives.

(10) Refer actual criminal or CI incidents to NCIS.

b. Commanding Officers will:

(1) Appoint a command InT Representative in writing and provide the designation letter to the NLSC InT Representative.

(2) Ensure all cleared military, civilian, and contractor personnel at the command complete InT awareness training as required by reference (a) (Navy eLearning: DON-CIAR-1.0-NCIS Counterintelligence and Insider Threat Awareness and Reporting; Waypoints: 00-DON-NCIS Counterintelligence and Insider Threat Awareness and Reporting Training). Training must be completed within 30 days of initial employment, entry-on-duty or following the granting of access to classified information and annually thereafter.

(3) Report potential command InT concerns or incidents, per enclosure (2) of reference (a), directly to the Navy InT Hub. Use OPNAV 5510/423 (Navy Insider Threat Report) to submit InT reports. Upon receipt of a response from the Navy InT Hub, report all mitigating actions taken within 30 days. Provide a copy of the InT report to the NLSC InT Representative.

(4) Submit an OPREP-3 message as required by reference (h). If an OPREP-3 message is required, ensure the Navy Hub is notified via separate correspondence of the reportable information contained in enclosure (2) of reference (a), and contact the Navy Hub to provide PII information regarding the subject(s) involved. Provide the NLSC InT Representative a copy of the OPREP-3 message as well as the PII information.

(5) Provide mitigations for identified InT behavior, keeping the NLSC InT Representative informed.

(6) Develop internal command reporting procedures as necessary.

(7) Refer actual criminal or CI incidents to NCIS.

c. All military, civilian, and contractor personnel in the NLSC enterprise will:

(1) Familiarize themselves with, and enforce the policies outlined in, this instruction.

(2) Report suspected InT behaviors to either the NLSC InT Representative or their command's designated InT Representative and Activity Security Manager per the reporting criteria of reference (a) enclosure (2). Alternatively, if time does not permit reporting to either the NLSC InT Representative or their command's InT Representative and Activity Security Manager, personnel may report directly to the Navy Hub via the following means:

<https://www.secnav.navy.mil/itp>, 703-695-7700, or [insiderthreat.fct@navy.mil](mailto:insiderthreat.fct@navy.mil); and back brief either the NLSC InT Representative or the command's InT Representative as soon as possible.

7. **Records Management.** 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 Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at

<https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

8. **Review and Effective Date.** Per OPNAVINST 5215.17A, NLSC 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 2016.

9. **Forms.** All referenced forms may be obtained by going to the OJAG Security SharePoint page [https://flankspeed.sharepoint-mil.us/sites/JAG\\_PORTAL\\_HOME/SitePages/OJAG-Security.aspx](https://flankspeed.sharepoint-mil.us/sites/JAG_PORTAL_HOME/SitePages/OJAG-Security.aspx).



DAVID G. WILSON

**Releasability and Distribution:**

This instruction is cleared for public release and is available electronically only, via Navy Judge Advocate General's Corps public website, <http://www.jag.navy.mil/instructions>

16 Jan 2025

## DEFINITIONS

Reference (a) is the Navy Insider Threat Program instruction. It provides the following guidance:

a. An insider is defined as any person with authorized access to any U.S. Government resource to include personnel, facilities, information, equipment, networks, or systems.

b. An insider threat is defined as a threat presented by a person who:

(1) Has, or once had, authorized access to information, a facility, a network, a person or a 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 may include physical harm to self or another in the workplace.