



DEPARTMENT OF THE NAVY  
COMMANDER  
NAVAL EDUCATION AND TRAINING COMMAND  
250 DALLAS STREET  
PENSACOLA, FLORIDA 32508-5220

NETCINST 5510.4  
N04  
14 Jan 2025

NETC INSTRUCTION 5510.4

From: Commander, Naval Education and Training Command

Subj: NAVAL EDUCATION AND TRAINING COMMAND INSIDER THREAT PROGRAM

Ref: (a) E.O. 13587  
(b) DoD Directive 5205.16 of 30 September 2014  
(c) SECNAVINST 5510.30C  
(d) OPNAVINST 5510.165B  
(e) SECNAVINST 5510.37A  
(f) CNO WASHINGTON DC 281639Z Jul 23 (NAVADMIN 170/23)  
(g) NETCINST 5214.1D

Encl: (1) Navy Insider Threat Potential Risk Indicators Reporting Criteria

1. Purpose. To establish the Naval Education and Training Command (NETC) Insider Threat Program (InTP) following the guidelines and procedures of references (a) through (g), publish policy, assign responsibilities, and institute the NETC Insider Threat Working Group (ITWG).

2. Background. Per reference (a), the President directed all agencies and organizations that "operate or access classified computer networks" to establish an InTP. Reference (b) provides further guidance on Department of Defense (DoD) requirements for InTPs to prevent, deter, and detect and mitigate the threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions and resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, kinetic violence, or through the loss or degradation of departmental resources or capabilities. Reference (c) ensures maximum uniformity and effectiveness in the application of personnel security program policies within the Department of the Navy (DON). The objective of the personnel security program is to authorize initial and continued access to classified information and initial and continued assignment to sensitive duties to those persons whose loyalty,

reliability, and trustworthiness are such that entrusting them with classified information or assigning them to sensitive duties are clearly consistent with the interests of national security. Reference (d) disseminates InTP guidance, issues policy, and assigns responsibilities. Reference (e) directed the DON to establish a single, consolidated DON Hub to gather, integrate, assess, and refer information derived from relevant authorized sources to identify potential InTs within the DON. Reference (f) delineates policy and guidance regarding the United States Navy Insider Threat Program. Reference (g) prescribes policy, responsibility, and guidance for Commander's Critical Information Requirements (CCIR) reporting to force development domain on events requiring notification to Commander, NETC and Headquarters (HQ) staff leadership.

### 3. Discussion

a. The security of our nation depends on our defense capabilities being in the right place, at the right time, with the right qualities and capacities. While executing NETC's mission, our people, facilities, technology, and information must be protected from insider threats.

b. InT Definition: An insider threat is a threat presented by a person who:

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

(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 another in the workplace.

c. InT behavior may include unacceptable conduct; violent outbursts; threatening comments or comments supporting enemy or terrorist actions, including those posted to social media; criminal arrests; unexplained or undocumented foreign travel and

contacts; or failure to consistently follow security regulations. Reporting criteria are listed in enclosure (1).

d. NETC InTP policies will leverage existing Federal laws, statutes, authorities, policies, programs, systems, architecture, and resources, and employ risk management principles, tailored to meet the distinct needs, mission, and systems of the NETC enterprise, and include appropriate protections for privacy, civil rights, and civil liberties. Actions taken in response to an InT may include, but are not limited to:

(1) Suspending or revoking physical access to sensitive, controlled, or restricted areas.

(2) Referring actual or suspected InT incidents to the Naval Criminal Investigative Service (NCIS) and NETC HQ InTP Program Manager (PM).

e. NETC HQ InTP PM. The InTP PM is functionally responsible for administering the InTP within NETC HQ and will:

(1) Act as the Commander's InTP representative for NETC.

(2) Develop and manage the InTP.

(3) Provide guidance and oversight to NETC domain echelon 3 commands.

(4) Facilitate coordination of InTP matters within the NETC HQ and domain.

(5) Have direct access and report to the commanding officer (CO) and activity security manager (ASM).

(6) Conduct continuous evaluation of personnel and investigate potential or actual InTs.

(7) Report actual or suspected incidents of InT activity to the commander as per guidance in reference (g), and ensure actual incidents are reported in the Defense Information System for Security (DISS). (Note: Statutory and administrative due

diligence is required as adverse information might impact an individual's ability to maintain security clearance eligibility. Only actual incidents may be reported in DISS.)

(8) Coordinate with local installation law enforcement for escort of personnel off the installation when notified of a proposed debarment, suspension, or termination of an individual from the command.

(9) Inform, educate, and consider coordinating activities among representatives from the following programs at NETC and their representative which make up the ITWG. The ITWG will work together as a team to discuss, mitigate, and to make recommendations to the commander on command insider threat activity. The ITWG members, led by the InTP PM, are as follows:

(a) ASM.

(b) Anti-terrorism Force Protection and Physical Security Officer.

(c) Chief Information Officer and Cyber Security Program Manager.

(d) Public Affairs Officer.

(e) Director, Human Resources.

(f) General Counsel and Force Judge Advocate.

(g) Inspector General.

(h) Senior Enlisted Advisor.

(i) Medical and mental health representative, as required.

(j) NCIS Agent, as required.

(10) Facilitate the protection of personnel, information, and facilities from InTs by developing standardized processes and procedures on:

(a) Training and awareness.

(b) Monitoring user and privileged user activities on all non-sensitive compartmented information systems in coordination with NETC Information Systems Security Manager (ISSM).

(c) Continuous evaluation of personnel.

(d) Detection, response, reporting, and investigation.

(e) Mitigation.

f. All NETC employees, to include contractors, military (active duty, reserve, guard), and civilian employees will conduct HQ monitoring and report to the NETC HQ InTP PM and NETC ISSM any threats and actions posing a risk to government information systems.

g. NETC ISSM will investigate, in conjunction with NETC InTP PM and ASM, incidents of actual or suspected unauthorized access into a government information technology system; intentional or negligent introduction of malware or unauthorized software, data corruption, alteration, or theft and, when appropriate, refer such cases for criminal investigation to NCIS.

(1) Initiate immediate action to isolate, mitigate, and prevent damage or loss to government information systems including suspension or removal of access to systems.

(2) Recommend, provide, or resource the appropriate software preventing, detecting, and monitoring for InTs at enterprise.

h. NETC InTP PM and NETC ASM will coordinate with NETC HQ CO regarding InT actions that may impact access, security clearance eligibility, and suspension or removal.

i. Supervisors at NETC will inform NETC ASM and InTP PM immediately of:

(1) Behavior that is considered disruptive, threatening, or falls within the criteria of an insider threat and has been reported verbally or in writing;

(2) Verbal or physical threats.

j. Commanders and COs of subordinate commands within the NETC domain will:

(1) Establish an InTP that emulates the NETC HQ InTP.

(2) Conduct oversight of subordinate command InTP programs.

(3) Submit a CCIR report to NETC HQ per references (f) and (g) to report incidents.

k. NETC personnel, including military, civilian, and contractor personnel will immediately report the following to the NETC InTP PM:

(1) Acts of violence or threats of violence toward a person or persons.

(2) All actual or suspected InT incidents listed in enclosure (1) of this instruction.

(3) Concerns about other employees who pose or could pose an InT.

(4) Adverse information that may affect their own security clearance eligibility. This information should also be reported to their respective personnel security specialists.

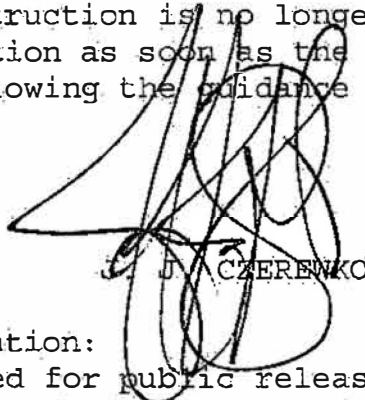
#### 4. Records Management

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 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>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

14 Jan 2025

5. Review and Effective Date. Per OPNAVINST 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, 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.



J. CZERENKO

Releasability and distribution:

This instruction is cleared for public release and is available electronically on the NETC public web site ([www.netc.navy.mil](http://www.netc.navy.mil)) or by e-mail at [netc-directives@us.navy.mil](mailto:netc-directives@us.navy.mil).

NAVY INSIDER THREAT POTENTIAL RISK INDICATORS REPORTING CRITERIA

**CRITERIA 1: SERIOUS THREATS**

a. Verbal or non-verbal threats to DON installations, facilities, personnel, missions, or resources.

(1) Direct, indirect, or veiled threats of harm or violence.

(2) Intimidating, belligerent, harassing, bullying, or aggressive behavior.

b. Threatening violence in the workplace.

(1) Numerous conflicts (negative interactions) with supervisors and other employees.

(2) Bringing an unauthorized weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to the use of guns.

(3) Statements showing fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a personal or professional problem, or statements indicating identification with perpetrators of workplace homicides.

c. Conveying a direct or veiled threat of violence to a third party.

d. Blatant or intentional disregard for the safety of others.

**CRITERIA 2: ALLEGIANCES AGAINST THE UNITED STATES AND TERRORISM**

a. Association with persons who are attempting to commit, or who are committing, any act of sabotage, treason, sedition, or other act whose aim is to overthrow the government of the United States or alter the form of government by unconstitutional means.



b. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

c. Association or sympathy with persons who are attempting to commit, or who are committing terrorism against the United States.

d. Expressing ill-will toward the government of the United States, the DON, or DON personnel.

**CRITERIA 3: ESPIONAGE AND FOREIGN CONSIDERATIONS**

a. Unreported contact with an individual who has known or suspected associations with a foreign intelligence entity or security organization.

b. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.

c. Unreported foreign travel and unreported foreign contacts.

d. Dual citizenship.

e. Unreported foreign interests, business, or property.

**CRITERIA 4: UNUSUAL BEHAVIOR AND SIGNS OF EXCESSIVE STRESS**

a. Extreme changes in behavior or personality.

(1) Behavior, including but not limited to, overly aggressive or angry language, delusional statements or paranoia, and increased isolation, which causes disruption or hostility in the work environment.

(2) Irresponsible, uncontrolled, violent, paranoid, emotionally unstable, or generally concerning behavior.

(3) An abrupt and significant change in an individual's appearance or behavior suggesting impaired judgment or stability.

(4) Apparent or suspected mental health issues where there is a reason to believe it may impact a DON-affiliated individual's ability to protect classified or controlled unclassified information.

(5) Stalking or surveilling an individual or individuals.

(6) Refusal to take an authorized polygraph examination.

**CRITERIA 5: CRIMINAL, VIOLENT, OR ABUSIVE CONDUCT**

a. Personnel investigated, arrested, or apprehended for incidents involving the loss of life.

b. Personnel investigated, arrested, or apprehended for incidents involving actual or suspected acts of violence, to include domestic battery, sexual assault, or child pornography.

c. Personnel investigated, arrested, or apprehended for incidents involving the illegal possession or transfer of weapons of mass destruction.

d. Personnel investigated, arrested, or apprehended for incidents involving the use of weapons or explosives.

e. Failure to follow a court order, to include violation of a restraining order or probation.

f. Statements indicating the individual is involved in criminal activity.

g. Wrongfully damaging or destroying property.

**CRITERIA 6: FINANCIAL CONSIDERATIONS**

a. Statements indicating financial hardship (e.g., high-value delinquent debt, bankruptcy, foreclosure, or high debt-to-income ratio).

b. Statements indicating desperation over family, financial, and other personal problems; potentially to the point of contemplating suicide.

- c. Unexplained affluence or excessive indebtedness.
- d. Excessive gambling.

**CRITERIA 7: SELF-DESTRUCTIVE BEHAVIORS OR OTHER BEHAVIORAL CONSIDERATIONS**

- a. Suicidal ideations or self-inflicted harm.
- b. Signs of alcohol abuse or intoxication on the job.
- c. Illegal use or misuse of drugs or controlled substances.
- d. Drug test failure.
- e. Arrest or criminal proceedings associated with legal or illegal substances.

**CRITERIA 8: SECURITY INFRACTIONS OR VIOLATIONS**

- a. A willful, intentional, or negligent compromise or loss of classified or controlled unclassified information.
- b. Purposeful mishandling of classified or controlled unclassified information.
- c. A security incident brought upon by the intentional or unintentional failure to comply with information security requirements.
- d. Non-compliance with rules or policy violations. An unwillingness to comply with rules and regulations or to cooperate with security requirements.
- e. Misuse of government travel card or DoD purchase card.
- f. Excessive physical access attempt denials.

**CRITERIA 9: MISUSE OF INFORMATION TECHNOLOGY**

- a. Deliberate or negligent misuse, to include malicious damage or destruction, of information technology systems or software.

- b. Unauthorized use of removable media.
- c. Use of account credentials by an unauthorized individual.

**CRITERIA 10: PERSONNEL SECURITY AND HUMAN RESOURCES  
CONSIDERATIONS**

- a. Any activity that raises doubts as to whether a DON-affiliated individual's continued national security eligibility is clearly inconsistent with the interests of national security.
- b. Intentional deception in an official process, to include falsifying hiring information.
- c. Failing to reveal all relevant facts, altering facts, or lying.
- d. Adverse clearance actions, such as suspension, revocation, or denial of a security clearance.
- e. The suspicious death of DON-affiliated personnel.
- f. The unexplained disappearance or unauthorized absence (more than 24 hours) of DON-affiliated personnel.
- g. Declining performance or poor performance rating.
- h. Excessive absences from work or absent without leave.
- i. Written reprimand, demotion, non-judicial punishment, suspension or other disciplinary action.
- j. Dishonorable discharge or anything other than honorable discharge.