BUMED INSTRUCTION 5510.9A

From: Chief, Bureau of Medicine and Surgery

Subj: BUREAU OF MEDICINE AND SURGERY INSIDER THREAT PROGRAM

(b) SECNAVINST 5211.5F
(c) DoD Directive 5205.16 of 30 September 2014
(d) E. O. 13587
(e) SECNAVINST 5510.37A
(f) OPNAVINST F3300.53C
(g) BUMEDINST 3300.1B
(h) SECNAVINST 5510.30C
(i) DoD Instruction O-2000.16 Volumes 1 and 2 of 20 November 2019

Encl: (1) Definitions and Acronyms
      (2) U.S. Department of Justice, Insider Threat
      (3) Asymmetric Warfare Group: Insider Threats in Partnering Environments

1. **Purpose.** To establish the Bureau of Medicine and Surgery (BUMED) Insider Threat Program (ITP) per references (a) through (i), publish policy, assign responsibilities, and institute the Navy Medicine Insider Threat Working Groups. Reference (a) is available at http://www.navfac.navy.mil/content/dam/navfac/Specialty%20Centers/Engineering%20and%20Expeditionary%20Warfare%20Center/DoD_Lock_Program/PDFs/UG-2040-SHR.pdf. This instruction is a complete revision and should be reviewed in its entirety.

2. **Cancellation.** BUMEDINST 5510.9.

3. **Scope and Applicability.** This instruction applies to all BUMED readiness and training commands, readiness and training units, commands, support commands; and is applicable to all appropriate BUMED departments, antiterrorism/force protection (AT/FP), counterintelligence, information assurance, law enforcement personnel, security, human resources, public affairs, legal, and other authorities and processes that impact or influence insider threat deterrence, detection, and mitigation capabilities.

4. **Background.** Per references (a) through (i), all readiness and training commands, readiness and training units, commands and activities are to establish an insider threat program to deter, detect and mitigate insider threats, and protect classified national security information. Unauthorized disclosures of classified information have caused significant damage to national
security and violent acts have resulted in loss of life and damage to operational resources. Reference (b) defines the Deputy Undersecretary of the Navy for Policy as the Department of the Navy ITP lead. Enclosure (1) defines definitions and acronyms found throughout this instruction.

5. Insider Threat Definition. Per reference (c) and (d), an insider threat is a person with authorized access, who uses that access wittingly or unwittingly to harm national security interests through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss of degradation of resources or capabilities. The term kinetic can include, but is not limited to, the threat of harm from sabotage or workplace violence.

6. Policy. BUMED 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 Navy 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. These policies must employ risk management principles, be tailored to meet the distinct needs, mission and systems of individual agencies, and must include appropriate protection for an individual’s privacy, civil rights and civil liberties.

7. Responsibilities

   a. Antiterrorism Executive Committee (ATEC BUMED-M4B) must:

      (1) Provide oversight and guidance to all BUMED subordinate commands.

      (2) Provide recommendations, prioritizations, planning, programming, information sharing, and policy for BUMED Headquarters, and BUMED subordinate commands.

      (3) Incorporate the Navy ITP into the ATEC charter.

      (4) Exercise oversight, management, and review all BUMED subordinate commands Navy ITP plans and programs.

      (5) Disseminate any pertinent insider threat information and training to the regional antiterrorism officers.


      (7) Per references (b) through (e), ensure corresponding programs are current and executable. At a minimum, the programs included in budget submitting office (BSO) 18’s ITP:
(a) AT/FP Program.
(b) Personnel and Industrial Security Program.
(c) Navy Key and Lock Program.
(d) Counterterrorism Program and Annual Training.
(e) Access Control Program.

b. **Deputy Chief, Total Force (BUMED-M1/7)** must ensure that insider threat information is included in all of the BSO-18 personnel accession screenings and personnel records. Training and Education (BUMED-M7B) will ascertain the appropriate education and training venues.

c. **Assistant Deputy Chief, Information Management and Information Technology, Chief Information Officer (BUMED-M6B)** will comply with references (a) through (i). BUMED-M6B must ensure all cyber and information systems requirements are in compliance with higher headquarters requirements and that annual user training is completed and documented. BUMED-M6B must also ensure all information systems possess proper protocols to mitigate susceptibility to an insider threat.

d. **Assistant Deputy Chief, Fleet Support and Logistics (BUMED-M4B)**, per references (b) through (d), must coordinate with the Special Assistant, Staff Judge Advocate (BUMED-M00J) to ensure input to, and oversight of, the Navy ITP in protecting and safeguarding all legal, civil, and privacy rights of BSO-18 personnel per reference (d).

e. **BUMED Medical Inspector General** will incorporate ITP inspection line items into the existing AT/FP inspection tool for inspection of this program.

f. Commanders, Naval Medical Forces, Commanders and Commanding Officers of Navy Medicine Readiness and Training Commands, Officers in Charge of all Navy Medicine Readiness and Training Units, labs, and facilities to include BUMED Headquarters and their detachments must meet the requirements of this instruction and ensure they:

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

(2) Are aware of high-risk behavior that can indicate a potential threat. A sample listing of these behaviors are listed below. This list is not all inclusive:

(a) Extremist or fascination with terrorist organizations.

(b) Abrupt change in personality or social engagement.

(c) Angry outburst or hateful comments about co-workers or organization.
(d) Reports of physical or cyber harassing and bullying.

(e) Significant interest in areas outside the scope of their duties.

(f) Working odd hours without authorization.

(g) Requesting access to information, systems, or facilities not associated with their duties.

(h) Remotely accessing the network at odd times or while on vacation.

(i) Unnecessarily copying or downloading sensitive information.

(j) Signs of drug use, alcohol abuse, or illegal activity.

(k) Financial difficulty or gambling addiction.

(l) Unexplained wealth or unusual foreign travel.

(m) Repeated rule violations.

(3) Establish clear guidelines for reporting suspicious behavior. Commands must develop their own reporting procedures, and ensure staff is trained and understands the reporting process. Commands are encouraged to consult the entities listed in subparagraphs 7f(3)(a) through 7f(3)(g) when developing their reporting procedures:

(a) Chain of Command

(b) Command security manager

(c) Command antiterrorism officer

(d) Human resources

(e) Naval Security Forces

(f) Naval Criminal Investigative Service special agent

(g) Command Staff Judge Advocate or legal officer

(4) Ensure reporting protects the privacy of all concerned.
(5) Account for public safety exceptions to statutes and regulations.

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

(7) Implement a system to collect and correlate data while, at all times protecting the privacy of those reporting and reported.

(8) Establish data retention and storage protocols.

(9) Develop and establish procedures for recommending an appropriate response.

(10) Regularly review regional AT/FP, physical security and cyber security instructions, training, and policy to ensure consistency with preventing insider threats. This must be accomplished at a minimum every 2 years.

(11) Develop an insider threat instruction which delineates specific responsibilities to subordinate commands.

(12) Ensure all insider threat information and or training is provided to subordinate commands. Leverage all government insider threat information and conduct counterintelligence training annually in conjunction with regional security managers and command information security officers. Enclosures (2) and (3) are examples of sources of training for the command staff.


(14) Establish a Navy insider threat working group. Incorporation of the Navy ITP into an existing Force Protection Board or Antiterrorism Working Group that meets at a minimum semi-annually is acceptable, per (f) through (i).

(15) Ensure all regional information systems officers and command level information security officers comply with this instruction and references (a) through (i).

(16) Verify the records of all new personnel accessions are appropriately screened and all necessary education and training has been completed.

(17) Develop guidance for all subordinate commands within their specific area of responsibility.
(18) Ensure all BUMED subordinate commands or activities have established a policy to review all program specific software and programs that non-U.S. citizens have access to. This review must occur, at a minimum, annually. Frequent spot checks to ensure the integrity of non-critical sensitive information are highly recommended.

g. Commanders, Naval Medical Forces, Commanders and Commanding Officers of Navy Medical Readiness and Training Commands, Officers in Charge of all Navy Medical Readiness and Training Units, labs, and facilities to include BUMED Headquarters and their detachments must ensure the identity of an individual reporting a potential insider threat to the command and the substance of information reported is limited to those who have a need-to-know. The ITP 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.

(1) Derogatory information acquired as the result of a suspected insider threat report should be shared only with those who have a need-to-know or an agency component in a position to confirm or deny an allegation. The information should be reviewed for credibility and accuracy prior to command administrative or disciplinary action. The ITP should also ensure that any inaccuracies it has found are remedied and corrections passed along to recipients of the erroneous data.

(2) Reported 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. Finally, it may be necessary to establish or amend an agency’s System of Records Notice (SORN) to ensure compliance with the Privacy Act of 1974.

(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 of the applicable privacy impact assessment(s), SORN(s), and departmental directive(s), instruction(s), and standard operating procedures.

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

(5) 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 danger to staff or beneficiaries.
8. **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 Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records Management Division portal page at [https://portal.secanv.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx](https://portal.secanv.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 Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records Management Division program office.

9. **Review and Effective Date.** Per OPNAVINST 5215.17A, BUMED-M4B 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.

10. **Information Management Control.** The reports required in paragraph 6f are exempt from reports control per Secretary of the Navy Manual 5214.1 of December 2005, part IV, paragraph 7c.

   [Signature]

   G. D. SHAFFER
   Acting

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site at, [http://www.med.navy.mil/directives/Pages/BUMEDIInstructions.aspx](http://www.med.navy.mil/directives/Pages/BUMEDIInstructions.aspx)
DEFINITIONS AND ACRONYMS

ATEC - Antiterrorism Executive Committee

AT/FP - Antiterrorism/Force Protection. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information.

ATO - Antiterrorism Officers. A position whose responsibility is to enact and manage the AT/FP program.

BUMED - Bureau of Medicine and Surgery

CI - Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

CO - Commanding Officer

IA - Information Assurance. Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.

ITP - Insider Threat Program

LE - Law Enforcement

MEDIG - Medical Inspector General

OIC - Officer-in-Charge

RISO - Regional Information Systems Officer

SORN - System of Records Notice
RECENT INSIDER THEFT CASES

Michael Mitchell, a sales clerk, and enginner, became disgruntled and was fired from his job based on poor performance. Mitchell signed statements affirming he had retained all proprietary information to his employer and was reminded of nondisclosure policies. However, Mitchell kept numerous computer files, entered into a consulting agreement with a rival Korean company, and provided trade secrets from his former employer to that company. In March 2010, he was sentenced to 18 months in prison and ordered to pay his previous employer over $187,000.

Shahin Jhaveri, a technical operations associate, gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and continued to the investor that the information he had taken from his employer was everything he needed to start the business. He confessed that he disregarded the actions to evade detection. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $9,000 fine, and a $100 Special Assessment.

David Yen Lee accepted a job on 27 February 2009 from a business competitor in China, but did not resign from his current employer until 16 March 2009. Lee admitted to downloading trade secrets from his employer’s secured computer system for several months prior to his resignation. The stolen trade secrets were worth between $7 million and $20 million. In December 2010, Lee was sentenced to 15 months in prison and three years supervised release.

Sergey Alisyarov, a computer programmer, worked for a company on Wall Street from May 2007 until June 2009. During his last few days at that company, he downloaded, and transferred 32 megabytes of proprietary computer codes—a theft that could have cost his

**THE INSIDER THREAT**

An introduction to detecting and deterring an insider spy

- Disgruntled
- Working odd hours
- Unexplained influence
- Unreported foreign travel

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company’s trade secrets.
PROTECT YOUR INTELLECTUAL PROPERTY

Thrift of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

PERSONAL FACTORS

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

- Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.
- Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.
- Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.
- Ideology/Identification: A desire to help the "underdog" or a particular cause.
- Divided Loyalty: Allogeance to another person or company, or to a country besides the United States.
- Advanced/Thrill: Want to add excitement to their life, like the clandestine activity; "James Bond wannabe."
- Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Se/Imager: An "above the rules" attitude, desire to reap rewards to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Advanced/Thrill.

Ingratitude: A desire to please or win the approval of someone who could benefit them in return. Expectation of feedback.

Compulsive and destructive behavior. Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

ORGANIZATIONAL FACTORS

Organizational situations may increase the ease to the thief:

- The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access to those who do not need it.
- Proprietary or classified information is not labeled as such, or is incorrectly labeled.
- The ease that someone may exit the facility (or network system) with proprietary, classified, or other protected materials.
- Underline procedures regarding working from home on projects of a sensitive or proprietary nature.
- The perception that security is lax and the consequences for theft are minimal or non-existent.
- Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.
- Employees are not trained on how to properly protect proprietary information.

BEHAVIORAL INDICATORS

Employees behaviors may be a clue that an employee is spying and/or methodically stealing from the organization:

- Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.
- Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
- Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Remotely accesses the computer network while on vacation, sick leave, or at other odd times.
- Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.
- Unexplained foreign contacts (particularly with foreign government officials or intelligence officials) or unexplained overseas travel.
- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained absences, delays being things that they cannot afford on their household income.
- Engages in auspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.
- Overwhelmed by job or career disappointments.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company’s intellectual property, its reputation, its financial well-being, and its future.

Seek assistance from trained counterintelligence experts such as the FBI. Should you be suspicious, the FBI will assist you in protecting your company, but will not always be able to provide assistance.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting due diligence will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If solicited to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars to you and your employees upon request.

### Cultural Awareness
- **DO NOT** use derogatory terms in any language (even in friendly conversations).
- **DO NOT** slander host nation or coalition partners (even if only jokingly).
- **DO NOT** physically harm host nation or coalition partners (except in self-defense).
- **DO NOT** put down or slander any religion.
- **ALWAYS** be courteous and fair-minded for host nation and coalition partner hospitality.
- **ALWAYS** attempt to understand cultural sensitivities of partner nation personnel.
- **ALWAYS** ensure our partners know that we are providing security to their nation together as one team.
- **REPORT ALL SUSPICIOUS ACTIVITY**

### Hints for Success
- Report.
- Establish a baseline attitude and demeanor for individuals.
- Show that you are a fellow soldier by your actions and speech.
- Treat individuals with respect.
- Screen.
- Build personal inte...