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

IN REPLY REFER TO
BUMEDINST 5510.9A
BUMED-M4
3 Jun 2021

BUMED INSTRUCTION 5510.9A

From: Chief, Bureau of Medicine and Surgery

Subj: BUREAU OF MEDICINE AND SURGERY INSIDER THREAT PROGRAM

Ref: (a) Naval Facilities Engineering Service Center User's Guide (UG-2040-SHR) July 2000
(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.

(6) Implement required training on the U.S. Department of Defense Center for Development of Security Excellence for Insider Threat Awareness training, http://cdsetrain.dtic.mil/itawareness/.

(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.

(13) Implement insider threat training using one of the insider threat courses: Navy eLearning, DON-CIAR-1.0 (NCIS Counterintelligence and Insider Threat Awareness and Reporting Training), at https://learning.nel.navy.mil/ELIAASv2p/, NCIS Counterintelligence and Insider Threat, or Joint Knowledge Online, J3O P-US1343-NCIS, Counterintelligence and Insider Threat, at https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf.

(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.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 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.

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/BUMEDInstructions.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

U.S. DEPARTMENT OF JUSTICE, INSIDER THREAT

RECENT INSIDER THEFT CASES

Michael Mitchell, a sales clerk and engineer, became disgruntled and was fired from his job based on poor performance. Mitchell signed statements affirming he had returned 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.

Shalin 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 confirmed to the investor that the information he had taken from his employer was everything he needed to start the business. He confessed that he disguised his actions to evade detection. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $5,000 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 Aleynikov, 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 employer millions of dollars. He hoped to use the computer codes at his new Chicago-based employer. He attempted to hide his activities, but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets and transportation of stolen property in foreign commerce.

Greg Chung spied for China from 1979-2006. Federal charges against Chung consisted of stealing trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He was an engineer that stole hundreds of thousands of documents. He traveled to China under the guise of giving lectures while secretly meeting with Chinese government officials and agents. He was also encouraged to use Chi Mak (see below) to transfer information back to China. Chung was arrested in February 2008 and in February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for 20 plus years. He most recently passed information on quiet electric propulsion systems for the next generation of US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other specific technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Chi Mak was convicted of conspiracy, attempting to violate export control laws, failing to register as an agent of a foreign government, and making false statements to investigators. He was sentenced to over 24 years in prison, and four members of his family received varying sentences of up to 10 years in prison.

For additional information, training, or assistance, contact the FBI.
www.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider–the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a "spy"–someone who is stealing company information or products in order to *benefit another organization or country.*

THE INSIDER THREAT

An introduction to detecting and deterring an insider spy

- Disgruntled
- Working odd hours
- Unexplained affluence
- 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

Theft 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: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/ Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

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 for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges 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.

Undefined policies 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

Some 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.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Short trips to foreign countries for unexplained or strange reasons.

Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Overwhelmed by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

YOU CAN MAKE A DIFFERENCE

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

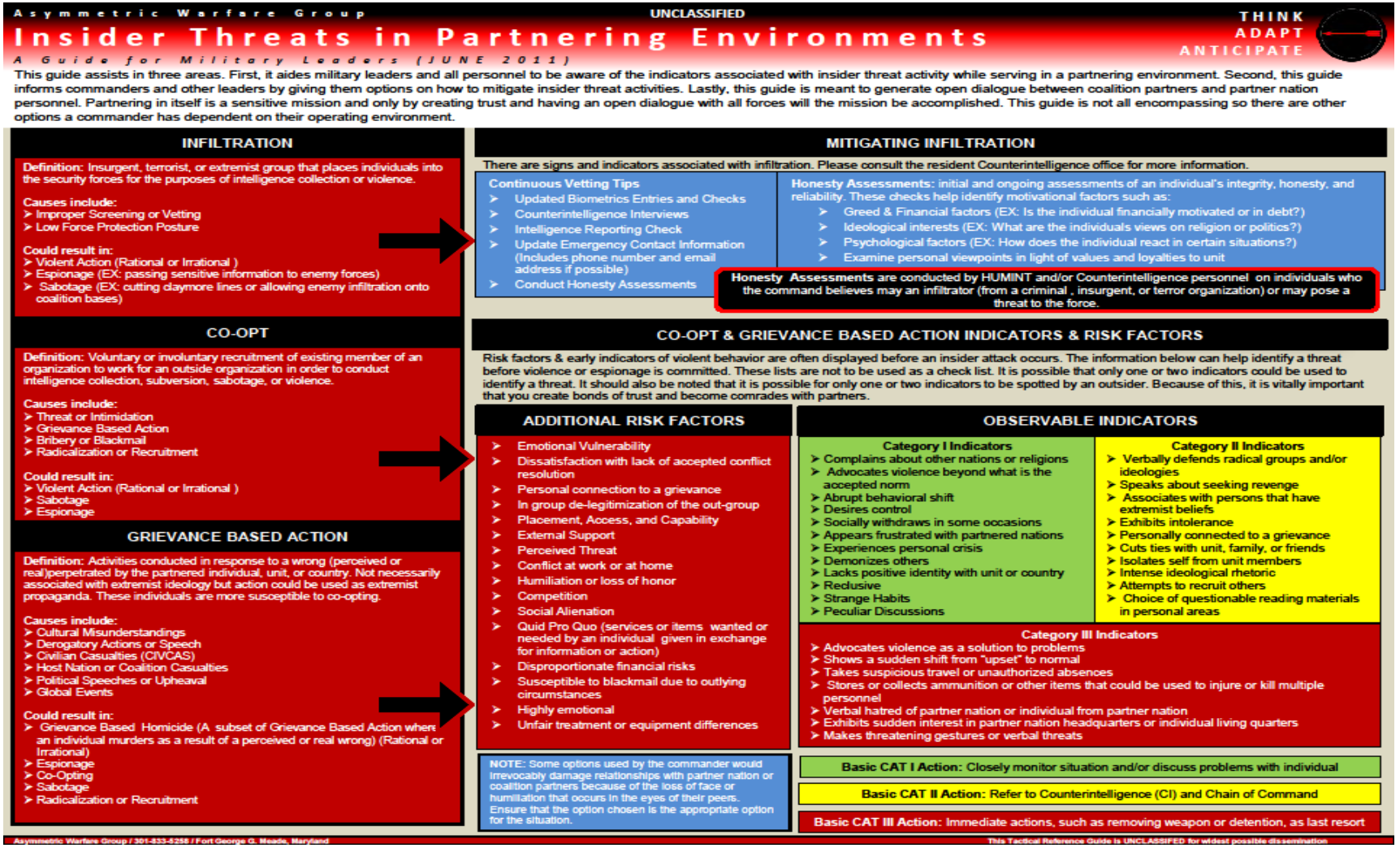
- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely 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. They are protecting their own jobs. Remind them that if they see something, to say something.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries 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 asked 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 for you and your employees upon request.

ASYMMETRIC WARFARE GROUP: INSIDER THREATS IN PARTNERING ENVIRONMENTS



Asymmetric Warfare Group — UNCLASSIFIED

Insider Threats in Partnering Environments

A Guide for Military Leaders (JUNE 2011)

THINK ADAPT ANTICIPATE

This guide assists in three areas. First, it aides military leaders and all personnel to be aware of the indicators associated with insider threat activity while serving in a partnering environment. Second, this guide informs commanders and other leaders by giving them options on how to mitigate insider threat activities. Lastly, this guide is meant to generate open dialogue between coalition partners and partner nation personnel. Partnering in itself is a sensitive mission and only by creating trust and having an open dialogue with all forces will the mission be accomplished. This guide is not all encompassing so there are other options a commander has dependent on their operating environment.

INFILTRATION

Definition: Insurgent, terrorist, or extremist group that places individuals into the security forces for the purposes of intelligence collection or violence.

Causes include:
- Improper Screening or Vetting
- Low Force Protection Posture

Could result in:
- Violent Action (Rational or Irrational)
- Espionage (EX: passing sensitive information to enemy forces)
- Sabotage (EX: cutting claymore lines or allowing enemy infiltration onto coalition bases)

CO-OPT

Definition: Voluntary or involuntary recruitment of existing member of an organization to work for an outside organization in order to conduct intelligence collection, subversion, sabotage, or violence.

Causes include:
- Threat or Intimidation
- Grievance Based Action
- Bribery or Blackmail
- Radicalization or Recruitment

Could result in:
- Violent Action (Rational or Irrational)
- Sabotage
- Espionage

GRIEVANCE BASED ACTION

Definition: Activities conducted in response to a wrong (perceived or real)perpetrated by the partnered individual, unit, or country. Not necessarily associated with extremist ideology but action could be used as extremist propaganda. These individuals are more susceptible to co-opting.

Causes include:
- Cultural Misunderstandings
- Derogatory Actions or Speech
- Civilian Casualties (CIVCAS)
- Host Nation or Coalition Casualties
- Political Speeches or Upheaval
- Global Events

Could result in:
- Grievance Based Homicide (A subset of Grievance Based Action where an individual murders as a result of a perceived or real wrong) (Rational or Irrational)
- Espionage
- Co-Opting
- Sabotage
- Radicalization or Recruitment

MITIGATING INFILTRATION

There are signs and indicators associated with infiltration. Please consult the resident Counterintelligence office for more information.

Continuous Vetting Tips
- Updated Biometrics Entries and Checks
- Counterintelligence Interviews
- Intelligence Reporting Check
- Update Emergency Contact Information (Includes phone number and email address if possible)
- Conduct Honesty Assessments

Honesty Assessments: initial and ongoing assessments of an individual's integrity, honesty, and reliability. These checks help identify motivational factors such as:
- Greed & Financial factors (EX: Is the individual financially motivated or in debt?)
- Ideological interests (EX: What are the individuals views on religion or politics?)
- Psychological factors (EX: How does the individual react in certain situations?)
- Examine personal viewpoints in light of values and loyalties to unit

Honesty Assessments are conducted by HUMINT and/or Counterintelligence personnel on individuals who the command believes may an infiltrator (from a criminal , insurgent, or terror organization) or may pose a threat to the force.

CO-OPT & GRIEVANCE BASED ACTION INDICATORS & RISK FACTORS

Risk factors & early indicators of violent behavior are often displayed before an insider attack occurs. The information below can help identify a threat before violence or espionage is committed. These lists are not to be used as a check list. It is possible that only one or two indicators could be used to identify a threat. It should also be noted that it is possible for only one or two indicators to be spotted by an outsider. Because of this, it is vitally important that you create bonds of trust and become comrades with partners.

ADDITIONAL RISK FACTORS
- Emotional Vulnerability
- Dissatisfaction with lack of accepted conflict resolution
- Personal connection to a grievance
- In group de-legitimization of the out-group
- Placement, Access, and Capability
- External Support
- Perceived Threat
- Conflict at work or at home
- Humiliation or loss of honor
- Competition
- Social Alienation
- Quid Pro Quo (services or items wanted or needed by an individual given in exchange for information or action)
- Disproportionate financial risks
- Susceptible to blackmail due to outlying circumstances
- Highly emotional
- Unfair treatment or equipment differences

OBSERVABLE INDICATORS

Category I Indicators
- Complains about other nations or religions
- Advocates violence beyond what is the accepted norm
- Abrupt behavioral shift
- Desires control
- Socially withdraws in some occasions
- Appears frustrated with partnered nations
- Experiences personal crisis
- Demonizes others
- Lacks positive identity with unit or country
- Reclusive
- Strange Habits
- Peculiar Discussions

Category II Indicators
- Verbally defends radical groups and/or ideologies
- Speaks about seeking revenge
- Associates with persons that have extremist beliefs
- Exhibits intolerance
- Personally connected to a grievance
- Cuts ties with unit, family, or friends
- Isolates self from unit members
- Intense ideological rhetoric
- Attempts to recruit others
- Choice of questionable reading materials in personal areas

Category III Indicators
- Advocates violence as a solution to problems
- Shows a sudden shift from "upset" to normal
- Takes suspicious travel or unauthorized absences
- Stores or collects ammunition or other items that could be used to injure or kill multiple personnel
- Verbal hatred of partner nation or individual from partner nation
- Exhibits sudden interest in partner nation headquarters or individual living quarters
- Makes threatening gestures or verbal threats

NOTE: Some options used by the commander would irrevocably damage relationships with partner nation or coalition partners because of the loss of face or humiliation that occurs in the eyes of their peers. Ensure that the option chosen is the appropriate option for the situation.

Basic CAT I Action: Closely monitor situation and/or discuss problems with individual

Basic CAT II Action: Refer to Counterintelligence (CI) and Chain of Command

Basic CAT III Action: Immediate actions, such as removing weapon or detention, as last resort

Asymmetric Warfare Group / 301-833-6258 / Fort George G. Meade, Maryland — This Tactical Reference Guide is UNCLASSIFIED for widest possible dissemination

Insider Threats in Partnering Environments *A Guide for Military Leaders (JUNE 2011)* **UNCLASSIFIED**

CULTURAL AWARENESS

- DO NOT use derogatory terms in any language (even in friendly conversation)
- 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 thankful for host nation and coalition partner hospitality
- ALWAYS attempt to understand cultural sensitivities of partnered nation personnel
- ALWAYS ensure our partners know that we are providing security to their nation together as one team

HINTS FOR SUCCESS

- Rapport
  - 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
  - Enroll all personnel into biometrics entering coalition bases
  - Secure mobile phones at entry control points or at designated areas (where possible and as mission requires)
- **REPORT ALL SUSPICIOUS ACTIVITY**

PREVENTIVE ACTIONS

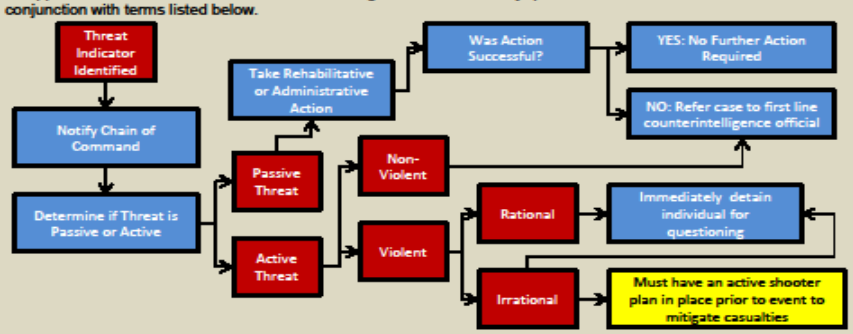
- Conduct random sweeps of installation to identify unauthorized personnel (Insider Threat Surge / Clean Sweep Operations)
- Develop workforce standards that mitigate risk, including additional security requirements, disciplinary procedures, and grievance resolution
- Develop training for reporting suspicious behavior
- Educate partners on how to identify observable indicators and assist in developing mechanisms to allow reporting internally and to other coalition partners
- Access control procedures and compartmentalization of critical information, activities, and physical areas
- Educate soldiers regarding the cultural differences by allowing the host nation to give cultural courses
- Establish confidential reporting procedures for threat indicators
- Use organic assets to collect information where there is a lack of Counterintelligence (CI) support (Every Soldier is a Sensor)
- Identify key personnel within the command structure that will carry weapons that are loaded at all times
- Develop roving guards that randomly check for loaded weapon s of all installation personnel (US and Partner)

ACCESS CONTROL MATRIX

Criteria	Level	Recommended Actions
➢ Successfully completes a force protection (FP) screening ➢ No connections to any insurgent, terrorist, or extremist group and/or personalities ➢ No reporting showing derogatory information ➢ No large debts identified (more than $100 USD) ➢ Has a requirement for such access	POTENTIAL Baseline for Access Control	Restricted Access / Can be unescorted
➢ Previous violations of installation policies / rules ➢ Has not been screened by FP personnel ➢ Suspected of corruption or illegal activity ➢ Uncorroborated or one-time reporting ➢ Family members identified as supporting illegal groups ➢ Failed vetting criteria used for maintaining or requesting access	MODERATE	Restricted Access / Must be escorted
➢ Theft or smuggling items on/off installation ➢ Efforts to access sensitive operational information ➢ Voices support or approval of insurgent, terrorist, or extremist groups ➢ Family members actively participating in illegal groups ➢ Selling / distributing drugs to installation personnel	HIGH	➢ Recommend firing & Biometrics Watchlist addition ➢ Pass REL dossier to host nation and coalition forces authority ➢ Temporary Removal
➢ Foreign intelligence agent or acknowledgement of foreign intelligence agent connections ➢ Latent fingerprints found on an object related to illegal groups ➢ Communicating information to third parties ➢ Reporting corroborated through intelligence	EXTREME	➢ Immediate removal, Biometrics Watchlist addition ➢ Possible Detention ➢ Pass REL dossier to host nation and coalition forces authority

INDICATOR DECISION CHART

The indicator decision chart is a guide for leaders to use if faced with an insider threat situation. This chart might not be applicable in all situations; consult counterintelligence if there are any questions. NOTE: Use this chart in conjunction with terms listed below.



ADDITIONAL REFERENCES

- **Army Counterintelligence Center:** http://acic.north-inscom.army.smil.mil/ho01.asp
- **902d MI Group Insider Threat:** http://acicportal.north-inscom.army.smil.mil/cira/default.aspx
- **Afghanistan Insider Threat:** http://www.afghan.centcom.smil.mil/intel/cj2x/ciit/default.aspx
- **Iraq Insider Threat:** http://cj2.s-iraq.centcom.smil.mil/CJ2X/Pages/default.aspx
- **USAREUR Threat Awareness and Reporting System (TARP):** http://intel.eur.aep.army.smil.mil/Ops/G2X/CI/saeda/default.aspx

ADDITIONAL INSIDER THREAT TERMS

- **Threat Indicator:** any observable action that displays violent behavior, abnormal disgruntlement, radicalization, or an extreme world view on religion or another type of ideology.
- **Passive:** someone who is aware of insider activity or threat but whose inactivity allows the action to continue
- **Active:** willing to provide information or perform actions; may be violent or non-violent
  - **Violent:** active insiders who use force; they may act rationally or irrationally
    - **Rational:** well thought out, violent course of action; possibly resulting in avoidance of capture
    - **Irrational:** Unplanned, emotional, and could involve collateral damage
  - **Non-Violent:** active insiders who are willing to provide information (espionage) or conduct subversion, sabotage, and will conceal their actions
- **Radicalization:** the process by which an individual, group, or mass of people undergoes a transformation from participating in the political process via a legal means to the use, or support of, violence for political purposes
- **Violent Extremist:** individuals who openly express their religious, political, or ideological views through violence or a call for violence
- **Mimicking:** a tactic used by the threat to gain access to personnel or facilities, normally off limits, by impersonating official personnel or soldiers (not addressed on this TRG)

Asymmetric Warfare Group / 301-833-8258 / Fort George G. Meade, Maryland — This Tactical Reference Guide is UNCLASSIFIED for widest possible dissemination