



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

Canc: SEP 2018

MCBul 5510
PPO
29 SEP 2017

MARINE CORPS BULLETIN 5510

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS INSIDER THREAT PROGRAM (MCInTP)

Ref: See enclosure (1)

Encl: (1) References
(2) Guidance on Identifying and Sharing Behaviors of Concern
(3) Glossary
(4) Definitions

1. Purpose. This Marine Corps Bulletin (MCBul) serves as guidance in vitalizing the MCInTP.

2. Cancellation. MARADMIN 187/15.

3. Background. In accordance with reference (a) and in response to unauthorized disclosures of national security information, espionage, terrorism, and violent acts resulting in damage to national security and loss of life and injury to personnel and property, reference (b) directs the establishment of and establishes minimum standards for insider threat programs across the Executive Branch. References (c) through (ao) provide amplifying instruction to promote the development of an effective and comprehensive insider threat program that protects United States Marine Corps (USMC) personnel, facilities, critical infrastructure, equipment, and information across all security domains. To implement these policies, the Marine Corps establishes and implements an enterprise-wide insider threat program, made up of multi-disciplinary, integrated, and collaborative capabilities and stakeholders. MCBul 5510 sets forth policy and assigns responsibilities to deter, detect, and mitigate the insider threat.

a. Insider. A person who has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position. These individuals include Active and Reserve Component (including National Guard) military personnel, civilian employees (including non-appropriated fund employees), and Department of Defense (DoD) contractor personnel; this includes officials or employees from federal, State, local, tribal and private sector entities affiliated with or working with DoD who have been granted access to classified information by DoD based on an eligibility determination made by DoD or by another federal agency authorized to do so.

b. Insider threat. The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage,

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The purpose of the MCInTP is to enhance commanders' risk management decisions. The desired end-state is to recognize when stressors and potentially risky behaviors first develop and interrupt the chain of events early that can lead to an adverse outcome; protect classified information, classified networks; and deter, detect, and mitigate insider threat, workplace violence, and other action(s) that may jeopardize individual readiness, unit readiness and mission accomplishment. We will help personnel Protect What We Have Earned.

(2) Concept of Operations. The MCInTP shall be a preemptive and analytical capability to identify potential insider threats; obtain assistance for individuals; or interdict efforts to cause harm to national security and Marine Corps installations, facilities, personnel, and property.

(a) It is critically important to the success of the MCInTP for leaders at all levels of command to follow the Marine Corps leadership traits and principles set forth in reference (ab), as they provide the best foundation for detecting, deterring, and mitigating insider threats. Know Your Marines and Look out for Their Welfare establishes the basis for making informed risk management decisions about potential and actual insider threats.

1. Leaders must make a conscientious effort to observe their personnel and recognize that an individual may have no malicious intent, but is in need of help.

2. Commanders who inspire commitment to shared core values and who demonstrate ways to engage productively with value conflicts, are best positioned to invite individuals in uniform and out of uniform to remain aligned with the Marine Corps and the Government's principles, thereby saving careers, saving lives, and protecting national security.

(b) There are unwitting insiders who can be exploited by others. Adversaries have become increasingly sophisticated in targeting U.S. interests, and an individual may be deceived into advancing adversaries' objectives without knowingly doing so.

(c) The MCInTP's focus will be on the following lines of effort:

1. Establish a Marine Corps Insider Threat Analysis Center (MCITAC). The MCITAC:

a. Provides an automation-assisted enterprise-level capability for managing insider threat information by integrating multi-disciplined and trained personnel, information systems and technologies, and business processes.

b. Integrates and centrally analyzes key threat-related information on potential insider threats who may pose a risk to personnel, facilities, infrastructure, networks, and national security information. MCITAC analyzes information and data derived from:

- (1) Counterintelligence (CI).
- (2) Security.
- (3) Cybersecurity.
- (4) Civilian and military human resources (HR) personnel management.
- (5) Workplace violence prevention.
- (6) Antiterrorism (AT) risk management.
- (7) Law enforcement (LE).
- (8) User activity monitoring (UAM) on DoD computer networks.
- (9) Continuous evaluation.
- (10) Other authorized sources.

c. Complies with requirements of references (a), (b), (f), (i), (k), and (l) while assessing information on potential insider threats to personnel, facilities, infrastructure, networks, and national security information, and ensuring adherence to whistle-blower, civil liberty, and privacy protections.

2. Achieve the following with respect to Director of Intelligence's (DIRINT's) Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) Insider Threat program (InTP):

a. Ensure that the MCISRE InTP is interoperable with the MCITAC to allow efficient sharing of information, potential insider threats, Tactics, Techniques and Procedures, and lessons learned where appropriate.

b. Ensure that, independent of its Intelligence Community (IC) responsibilities, the MCISRE InTP functions as a supporting effort to the MCInTP and MCITAC.

3. Expand employment of Marine Corps classified network UAM and analysis.

4. Improve and refine security processes, systems, and information sharing procedures for CI, personnel security and LE, and information assurance information indicative of an insider threat.

5. Integrate existing capabilities to better detect, analyze and respond to activity and information indicative of an insider threat.

(d) The MCInTP's essential tasks shall be implemented in accordance with reference (ae).

b. Tasks

(1) Deputy Commandant for Plans, Policies, and Operations (DC PP&O) shall:

- (a) Serve as the Senior Executive and advocate for the MCInTP.

(b) Serve as the Commandant's Principal Member to the Department of the Navy (DON) Insider Threat Program Senior Executive Board (DON ITP SEB).

(c) Appoint the Senior Official(s) and Office of Primary Responsibility accountable for the MCInTP. Their responsibilities will include:

1. Establish, provide oversight, and manage the MCInTP across all mission areas, programs, activities, processes and procedures.

2. Develop and promulgate MCInTP policy and an implementation plan in accordance with references (a) through (ao).

3. Provide oversight for the integration of MCInTP activities with other DoD and DON insider threat programs.

4. Provide the Marine Corps representative(s) to DoD, DON and interagency forums engaged in countering insider threats.

5. Serve as the Principal Member to the DON ITP SEB in the Senior Executive's absence.

6. Serve as a Marine Corps representative (Advisory Member) to the DON ITP SEB.

7. Establish a MCITAC to integrate and manage insider threat information.

8. Ensure coordination with the Deputy Commandant for Information (DC I) and integration of Marine Corps Information Operations Center and Marine Corps Cyberspace Operations Group activities with the MCITAC.

9. Establish a Marine Corps enterprise-level MCInTP Executive Steering Group (ESG) to serve in conjunction with the Protection ESG and in accordance with reference (x).

10. Provide oversight and leadership for the Marine Corps Insider Threat Working Group (MCITWG). Annually review the policy set forth in reference (y) for currency and relevance.

11. Develop a Memorandum of Agreement between the Naval Criminal Investigative Service (NCIS) and the MCITAC to establish the framework, terms, responsibilities, and procedures for sharing investigative, security clearance, and other relevant information.

(2) Deputy Commandant for Combat Development and Integration shall:

(a) In coordination with DC PP&O, conduct a Capabilities Based Assessment (CBA) for insider threat.

(b) In coordination with NCIS and DIRINT, develop insider threat and CI awareness and reporting training for all Marine Corps personnel, either through instructor-led or web-based courses to include:

1. Cornerstone: The Commandant's Combined Commandership Course.

2. The Basic School.

3. Expeditionary Warfare School.
4. Command and Staff College.
5. Top Level School.
6. Senior Enlisted Professional Military Education Course.
7. First Sergeants Course.
8. First Sergeant/Master Sergeant Regional Seminars.
9. Advance Course.
10. Career Course.
11. Sergeants Course.
12. Corporals Course.
13. Lance Corporal Leadership Ethics Seminar.

(3) Deputy Commandant for Manpower and Reserve Affairs shall:

(a) Serve as a Marine Corps representative (Advisory Member) to the DON ITP SEB.

(b) Provide a GO/Senior Executive Service (SES) representative to the MCInTP ESG.

(c) Provide a representative (Core member) to the MCITWG.

(d) Ensure that the MCITAC receives access to HR data streams and records for cleared personnel to the extent appropriate and consistent with applicable laws, policies, regulations, and orders.

(e) Incorporate insider threat requirements into planning, programming, and budgeting as applicable to support the MCInTP.

(4) Deputy Commandant for Programs and Resources shall incorporate insider threat requirements into planning, programming, and budgeting as applicable to support the MCInTP.

(5) Deputy Commandant for Installations and Logistics (DC I&L) shall:

(a) Establish an Insider Threat Program at each Marine Corps installation, appoint an Insider Threat Program Manager and levy these requirements down to subordinate commands. Recommend the Command Security Manager serve as the Insider Threat program manager based on established connections with the Continuous Evaluation Program (CEP) and training received at the Marine Corps Security Management Course. Additional training can be accessed through the Center for Development of Security Excellence (CDSE) website, <http://www.cdse.edu/toolkits/insider/>.

(b) The program manager must have direct and unfiltered access to the commanding officer and if not a member of the Force Preservation Council (FPC), should provide training to the FPC on identification of warning signs/indicators of potential insider threat behaviors of concern.

(c) Ensure subordinate commands provides insider threat identification training to their FPCs.

(6) DIRINT shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Core member) to the MCITWG.

(c) In coordination with NCIS, develop insider threat and CI Awareness and Reporting training for all Marine Corps personnel, either through instructor-led or web-based courses.

(d) Establish and implement MCInTP initiatives to identify and counter espionage, international terrorism, and the CI insider threat in accordance with references (j) through (p).

(e) Develop and recommend processes, procedures, and tools, to include the use of commercial-off-the-shelf technologies, to enhance the quality of CI capabilities and activities to counter insider threats.

(f) Ensure that the MCITAC receives access to CI data streams and records to the extent appropriate and consistent with applicable laws, policies, regulations, and orders.

(g) In accordance with references (j) through (p), develop and implement policy for the initiation, conduct, and oversight of CI activities to support the identification, neutralization, and exploitation of the insider threat.

(h) Incorporate insider threat mitigation requirements into Marine Corps CI resource planning, readiness assessments, and inspection procedures. Direct resource decisions, including manpower, for applicable operations, missions, and functions supporting insider threat mitigation.

(7) Director, Command, Control, Communications and Computers shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Core member) to the MCITWG.

(c) Develop and implement policy and strategy, to include audit and user activity monitoring standards, to counter insider threats on Marine Corps information networks to include:

1. Secure Internet Protocol Router.

2. Non-Secure Internet Protocol Router.

(d) Ensure the MCInTP has access to appropriate data streams and records to the extent consistent with applicable laws, policies, regulations, and orders.

(e) Incorporate insider threat cyber-based requirements into planning, programming, and budgeting as applicable to support the MCInTP.

(f) Conduct periodic evaluation and reviews of the insider threat mission area and cyber capability, capacity seams, gaps, and resource planning.

(g) Provide resource and acquisition guidance necessary for MCInTP completeness and effectiveness. This includes, but is not limited to, advocating for resourcing for insider threat or other IA programs that would effectively support a holistic MCInTP.

(h) Receive and implement, as appropriate, recommended changes to the MCInTP information technology capabilities from DoD and DON.

(i) Set standards for network security, operational performance, compliance, configuration control, and certification and accreditation to mitigate insider threat risk across the Marine Corps portion of the DoD information networks.

(8) Commanders, Marine Forces shall:

(a) Establish an Insider Threat Program, appoint an Insider Threat Program Manager and levy these requirements down to subordinate commands. Recommend the Command Security Manager serve as the insider threat program manager based on the established connection with the CEP and training received at the Marine Corps Security Management Course. Additional training can be accessed through the CDSE website, <http://www.cdse.edu/toolkits/insider/>.

(b) The program manager must have direct and unfiltered access to the commanding officer and if not a member of the FPC, should provide training to the FPC on identification of warning signs/indicators of potential insider threat behaviors of concern.

(c) Ensure subordinate commands provide insider threat identification training to their FPCs.

(d) Ensure collaboration and interaction with the Chaplain consistent with appropriate policy and instructions.

(e) Report insider threats (actual and potential) through the chain of command to the appropriate agency via established protocols and methods.

(9) Commander, Marine Corps Systems Command shall:

(a) Ensure the appropriate contract documents (e.g., Statement of Work, Performance Work Statement and Department of Defense Contract Security Classification Specification - DD 254) incorporate provisions that support Marine Corps insider threat policy enforcement.

(b) Ensure contracting officers coordinate closely with the MCInTP Manager to enforce Marine Corps insider threat requirements involving access to information, operations of networks owned by the Marine Corps, and insider threat training and reporting requirements.

(10) Staff Judge Advocate to the Commandant (SJA) shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Core member) to the MCITWG.

(c) Serve as a Marine Corps representative (Advisory Member) to the DON ITP SEB.

(d) Provide advice and assist in the development of policy related to MCInTP operations, information sharing with other DoD components, and other matters within the SJA's cognizance in accordance with SECNAVINST 5430.25E, SECNAVINST 2430.27D, and MCO P5800.16A (LEGADMINMAN).

(11) Office of Marine Corps Communication shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Core member) to the MCITWG.

(c) Maintain and update the Marine Corps Social Media Handbook with appropriate insider threat information.

(12) Medical Officer of the Marine Corps shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Advisory member) to the MCITWG.

(c) Provide medical and psychological expertise to the MCInTP including advice pertaining to clinical issues relevant to the behaviors observed, and mitigation of potential insider threat activities in coordination and communication with the MCITAC consistent with applicable laws, policies, regulations, and orders.

(d) Identify and provide the MCITAC access to information as authorized, consistent with applicable laws, policies, regulations, and orders, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA).

(13) Inspector General of the Marine Corps shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Advisory member) to the MCITWG.

(c) Facilitate independent assessments of the implementation of the MCInTP.

(14) Director, Commandant of the Marine Corps Safety Division shall ensure the next revision of MCO 1500.60 specifically addresses the role of Insider Threat Program Manager in the FPC process.

(15) Counsel to the Commandant (CL) shall:

(a) Provide a GO/SES representative to the MCInTP ESG.

(b) Provide a representative (Core member) to the MCITWG.

(c) Serve as a Marine Corps representative (Advisory member) to the DON ITP SEB.

(d) Provide advice and assist in development of policy related to security programs and functions, intelligence and cyber law, civilian personnel actions, acquisitions, and other matters within the cognizance of the Navy Office of General Counsel.

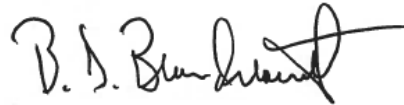
5. Administration and Logistics

a. Privacy Act Statement. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The DON recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities will be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII will be in accordance with the Privacy Act of 1974, as amended (reference (ag) and implemented per reference (af)).

b. Records Management. Records created as a result of this Bulletin shall be managed according to National Archives and Records Administration approved dispositions per reference (ah) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium.

6. Reserve Applicability. This Bulletin is applicable to the Marine Corps Total Force.

7. Cancellation Contingency. This Bulletin is cancelled one year from the date of publication or when incorporated as a Marine Corps Order, whichever occurs first.



B. D. BEAUDREULT
Deputy Commandant for
Plans, Policies, and Operations

Distribution: PCN 10208490900

- Ref:
- (a) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 07,2011
 - (b) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21,2012
 - (c) Executive Order 10450, "Security Requirements for Government Employment," April 27,1953
 - (d) Executive Order 12829, "National Industrial Security Program (as amended)," December 16,1993
 - (e) Executive Order 12968, "Access to Classified Information," August 02,1995
 - (f) Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information (as amended)," September 29,2016
 - (g) Executive Order 13526, "Classified National Security Information," December 29,2009
 - (h) Executive Order 12333, "United States Intelligence Activities (as amended)," August 04,2008
 - (i) DoD Directive 5205.16, "The DoD Insider Threat Program, 30 September 2014 Incorporating Change 1," Effective January 25,2017
 - (j) DoD Directive 5240.02, "Counterintelligence (CI)," March 17,2015
 - (k) DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 08,2016
 - (l) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR), W/Ch 1," May 30,2013
 - (m) DoD Instruction 5240.16, "Counterintelligence Functional Services (CIFS), W/Ch 1," October 15,2013
 - (n) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries, W/Ch2," October 15, 2013 (NOTAL)
 - (o) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat, W/Ch 1," October 15, 2013
 - (p) DoD Manual 5105.21-V3, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration Of Personnel Security, Industrial Security, and Special Activities," October 19,2012
 - (q) SECNAVINST 5510.37
 - (r) SECNAV M-5510.30
 - (s) OPNAVINST 5510.165A, "Navy Insider Threat Program," October 01,2015
 - (t) 2014 Guide to Accompany the National Insider Threat Policy and Minimum Standards, September 2014 (NOTAL)
 - (u) FBI Office of General Counsel, Summary of Federal Citations for the National Insider Threat Task Force
 - (v) CNSSD 504, "Protecting National Security Systems from Insider Threat of January 2012" (NOTAL)
 - (w) Volume 81, "Federal Register, Section 31614, Privacy Act of 1974; System of Records, Notice to Add New System of Records," May 19,2016
 - (x) Volume 81, "Federal Register, Section 65631, Privacy Act of 1974; System of Records, Notice to Alter a System of Records," September 23, 2016.
 - (y) Volume 81, "Federal Register, Section 71378, Privacy Act Exemption Rule for DoD Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records Systems," October 17, 2016

- (z) "Charter for the USMC Mission Assurance Operational Advisory Group (MA OAG)," November 14,2012
- (aa) "Marine Corps Insider Threat Working Group (MCITWG) Charter," October 16,2013
- (ab) MCRP 6-11B w/Ch1
- (ac) MCO 5580.3
- (ad) MCO 1500.60
- (ae) "Marine Corps Insider Threat Program Implementation Plan," February 2016
- (af) SECNAVINST 5211.5E
- (ag) 5 U.S.C.552a
- (ah) SECNAV M-5210.1
- (ai) ICD 502, "Integrated Defense of the Intelligence Community Information Environment," March 11,2011
- (aj) ICD 700, "Protection of National Intelligence," June 7,2012
- (ak) ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented information and Other Controlled Access Program Information," October 01,2008
- (al) ICPG 704.1, "Personnel Security Investigation Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 02, 2008
- (am) ICPG 704.2, "Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 02,2008
- (an) (U//FOUO) Intelligence Community Standard (ICS) 500-27, Collection and Sharing of Audit Data, June 2,2011 (NOTAL)
- (ao) (U//FOUO) ICS 700-2, Use of Audit Data for Insider Threat Detection, June 2,2011 (NOTAL)

GUIDANCE ON IDENTIFYING AND SHARING BEHAVIORS OF CONCERN

1. Identifying and sharing behaviors of concern requires recognition of potential indications and confidence that concerns can be reported and handled appropriately.

a. The list is not exhaustive, nor is it a checklist, but provides possible behaviors and activities that may be reported if an individual is exhibiting actions that cause concern.

b. These indicators were derived from multiple sources.

2. Possible behaviors of concern with respect to the security of classified information or networks include those that would impact a person's suitability, reliability, or trustworthiness for access to classified national security information. There are thirteen guidelines or interests described in reference (am) which can impact a person's suitability, reliability and trustworthiness. These are:

a. Allegiance to the United States.

b. Foreign Influence.

c. Foreign Preference.

d. Sexual Behavior.

e. Personal Conduct.

f. Financial Considerations.

g. Alcohol Consumption.

h. Drug Involvement.

i. Psychological Conditions.

j. Criminal Conduct.

k. Handling of Protected Information.

l. Outside Activities.

m. Use of Information Technology Systems.

n. Possible behaviors or indicators impacting these guidelines are provided in reference (am).

3. Possible indications, behaviors or activities of concern with respect to threats to classified information or systems, workplace violence, or other physical/kinetic threats include:

a. Direct, indirect, or veiled threats of harm or violence.

b. Intimidating, belligerent, harassing, bullying, or aggressive behavior.

c. Numerous conflicts with supervisors and other employees.

d. Bringing a weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to guns, or unusual fascination with weapons.

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

f. Statements showing fascination with incidents of workplace violence that is so unusual as to indicate potential criminal activity, statements indicating approval of the use of violence to resolve a problem, or statements indicating identification with perpetrators of workplace homicides.

g. Statements indicating desperation.

h. Pending or recent job layoff.

i. Drug/alcohol abuse.

j. Extreme changes in behavior, personality, or performance.

k. Acquisition of multiple weapons.

l. Escalation in target practice and weapons training.

m. Menacing actions with weapons.

n. Interest in explosives.

o. Interest in previous shootings or mass attacks.

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

q. Physical assault or physical violence.

r. Physical restraint or confinement.

s. Stalking or surveillance of individual(s).

t. Damages or destroys property.

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

v. Disruptive, aggressive, or angry language.

w. Poor work performance.

x. Disciplinary problems at work site.

y. Commission of a violent misdemeanor or felony at work site.

z. Delusional statements or paranoid ideas.

aa. Development of a personal grievance.

ab. Increased isolation.

ac. Odd or bizarre behavior.

ad. Loss of personal relationship (divorce, breakup, family member death).

ae. Depressed mood.

af. Suicidal ideation expressed.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

AT	Antiterrorism
CEP	Continuous Evaluation Program
CI	Counterintelligence
DC I	Deputy Commandant for Information
DC PP&O	Deputy Commandant, Plans, Policies, and Operations
DIRINT	Director of Intelligence
DoD	Department of Defense
DON	Department of the Navy
DON ITP SEB	Department of the Navy Insider Threat Program Senior Executive Board
ESG	Executive Steering Group
FPC	Force Preservation Council
HR	Human Resources
INTP	Insider Threat Program
LE	Law Enforcement
MCBUL	Marine Corps Bulletin
MCInTP	Marine Corps Insider Threat Program
MCISRE	Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise
MCITAC	Marine Corps Insider Threat Analysis Center
MCITWG	Marine Corps Insider Threat Working Group
NCIS	Naval Criminal Investigative Service
PII	Personally Identifiable Information
SCI	Sensitive Compartmented Information
SES	Senior Executive Service
SJA	Staff Judge Advocate to the Commandant
UAM	User Activity Monitoring
USMC	United States Marine Corps

DEFINITIONS

1. For purposes of this Bulletin:

a. Access. The ability or opportunity to gain knowledge of classified information.

b. Classified information. Official information that has been determined pursuant to Executive Order 13526, or any successor order, Executive Order 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in documentary form.

c. Cleared employee. A person or employee who has been granted access to classified information or who has been designated to hold a sensitive position in accordance with reference (c), Executive Order 10450, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces. As used in this Bulletin, the term 'employee' includes an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

d. Continuous Evaluation. The process by which all individuals who have established security clearance eligibility are monitored to assure they continue to meet the loyalty, reliability and trustworthiness standards expected of individuals who have access to classified information. The monitoring process relies on all personnel within a command to report questionable or unfavorable security information that could place in question an individual's loyalty, reliability, or trustworthiness.

e. Counterintelligence (CI). 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.

f. Counterintelligence (CI) Insider Threat. A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of a Foreign Intelligence Entity.

g. Damage to the National Security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

h. DD 254. The intention of a DD 254 is to convey security requirements, classification guidance and provide handling procedures for classified material received and/or generated on a classified contract.

(1) DD 254 is a resource for providing security requirements and classification guidance to a contractor.

(2) DD 254 is a U.S. publication referenced in the DFAR and applied to contracts involving access to classified information by U.S. contractors.

(3) If the contract is with non-U.S. Industry (foreign governments, cleared foreign companies or international organizations) additional guidance is on a case-by-case basis.

(a) The Industrial Security Implementing Agreement (to the General Security of Military Information Agreement) is the overarching authority for the bilateral protection of classified information with foreign governments.

(b) Any guidance provided to contractors to explain protection requirements for classified information exchanged under bilateral agreements must be conveyed through security contract clauses, and not a DD 254.

i. Detect. To discover or determine the existence, presence, or fact of.

j. Deter. To turn aside, discourage, or prevent from acting.

k. Implementation. The act of accomplishing some aim or executing some order.

l. Insider threat response action(s). Activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. An inquiry or investigation pursuant to insider threat response actions can be conducted under the auspices of CI, security, LE, or Inspector General elements, depending on statutory authority and internal policies governing the conduct of such activity in each agency.

m. Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) Insider Threat Program (InTP). In accordance with references (a) through (h), and (ai) through (an), DIRINT, as the Commandant of the Marine Corps appointed Head of an Intelligence Community Element, operates a complementary and mutually supporting, full capability InTP focused on the MCISRE and the Marine Corps Sensitive Compartmented Information indoctrinated population.

n. Mitigate. To cause to become less harsh or hostile.

o. Senior Official. The DoD official, designated by a DoD Component head, that is responsible for the direction, management, and oversight of the component's insider threat program.

p. Unauthorized disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

q. User Activity Monitoring. The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations.

r. Violence. The intentional and unlawful act, threatened or actual, against oneself, another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological, or physical harm.

s. Workplace. The workplace is any location either permanent or temporary where an employee performs any work related task and includes, but is not limited to, all common areas on a Marine Corps installation, unit spaces/buildings/structures, schools, recreational areas/facilities, fitness centers, parking lots, athletic fields, roadways, bachelor enlisted quarters, Marine Corps Exchanges, and training areas.

t. Workplace violence. Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or threatening, disruptive behavior that occurs at or outside the work site.