UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION
MARINE CORPS BASE QUANTICO
3250 CATLIN AVENUE
QUANTICO, VIRGINIA 22134-5001

MCINCR-MCBQO 5510.1
B 054
APR 29 2022

MARINE CORPS INSTALLATIONS NATIONAL CAPITAL REGION-MARINE CORPS BASE QUANTICO ORDER 5510.1

From: Commander, Marine Corps Installations National Capital Region-Marine Corps Base Quantico
To: Distribution List

Subj: COUNTER INSIDER THREAT PROGRAM (CInTP)

Ref: (a) MCO 5510.21
(b) MCO 1500.60
(c) SECNAVINST 5211.5F
(d) SECNAV M-5210.1

Encl: (1) CInTP Insider Threat Review Board Charter
(2) CInTP Risk Indicators
(3) CInTP Notification and Reporting
(4) CInTP Review Board Process

1. Situation. Reference (a) establishes policy and assigns responsibilities to prevent, deter, detect, and mitigate insider threats. This order establishes policy, formalizes procedures, assigns responsibilities, and implements control measures for the Marine Corps Installations National Capital Region-Marine Corps Base Quantico (MCINCR-MCBQ) Counter Insider Threat Program (CInTP).

a. This Order does not supersede:

(1) Authorities and policies of the Office of the Director of National Intelligence regarding the protection of sensitive compartmentalized information and special access programs for intelligence.

(2) Applicable law, regulation, and policy governing access to, or dissemination of law enforcement (LE), LE sensitive or classified LE information.

(3) Suspicious activity reporting and dissemination requirements.

(4) Applicable law, regulation, and policy governing counterintelligence (CI) and other intelligence activities.

(5) Requirements to refer information on criminal or counter intelligence allegations involving personnel affiliated with Department of Defense, Department of the Navy, or any property or programs under the control or authority of the Marine Corps to the Naval Criminal Investigative Service (NCIS). Such information shall be submitted as expeditiously as possible. Coordination and notification by Marine Corps Law Enforcement Agencies for referral to NCIS shall not be delayed for any improper purpose, to include inquiry, adjudicative, investigative, and other administrative actions for matters that fall within the jurisdiction of NCIS.

b. This Order reinforces accountability. All Marine Corps personnel, civilians, and contractors who have access to Marine Corps resources, are responsible for notifying appropriate leadership of concerning activity and behavior that could cause harm to national security.

2. Cancellation. MCINCR-MCBQO 5580.1A.

3. Mission. MCINCR-MCBQ establishes an integrated set of CInTP policies and procedures to prevent, deter, detect, and mitigate insider threats before damage is done to national security, personnel, resources, or capabilities.

4. Execution

a. Commander's Intent. To develop and implement a CInTP that allows stressors and concerning behaviors to be identified early and proactively. Recognition of the warning signs and behavioral indicators of a potential insider threat and notification is foundational to the success of the program and requires all Marines and employees to take this responsibility seriously. Once identified, the behaviors will be evaluated and courses of action will be identified to interrupt the chain of events and prevent an adverse outcome.

b. Concept of Operations

(1) The MCINCR-MCBQ CInTP consists of four phases: Training, Identification, Reporting, and Response.

(a) Training. MCINCR-MCBQ will create a culture of counter insider threat awareness and deterrence by providing training and education, emphasizing that it is an employee's duty and responsibility to notify appropriate leadership of suspicious behaviors and activities. All personnel must attend, every calendar year, the Counter Intelligence Briefing. The brief is scheduled and managed by the MCINCR-MCBQ Command Security Office, is conducted by NCIS, and consists of the following:

1. The importance of detecting potential insider threats and reporting suspected activity to insider threat personnel or other designated officials.

2. Methodologies of adversaries to recruit trusted insiders and collect classified information.

3. Indicators of insider threat behavior and procedures to report such behavior.

4. CI and security reporting requirements, as applicable.

5. Additional training is found at the Center for Development of Security Excellence website, http://www.cdse.edu/toolkits/insider.

(b) Identification. Although no single behavior or action can predict insider threat or activity with certainty, when such events occur, witnesses and victims often report they noticed changes in the individual's behavior, mood, and performance prior to the event. Enclosure (2) provides risk indicators of potentially concerning behaviors and activities.

(c) Reporting. Reporting behaviors of concern is necessary to determine the severity of the threat and appropriate response options. Reports

of insider threat behavior through continual vetting may also be received from the Service Analysis Section, Department of the Navy Analytic Hub. Enclosure (3) outlines notification and reporting processes and procedures.

(d) Response

1. IAW reference (b), reports of concerning behavior of active duty military personnel and International Military Students (IMS) are addressed through their respective Command's Force Preservation Council (FPC).

2. Reports of concerning behavior of Federal government employees are addressed by either their tenant command CInTP or the MCINCR-MCBQ Insider Threat Review Board. If the tenant command does not possess an established CInTP, then a request for Insider Threat Review Board support will be requested via the MCINCR-MCBQ Chief of Staff.

3. Reports of concerning behavior of contractor personnel are addressed by either their tenant command CInTP or the MCINCR-MCBQ Insider Threat Review Board. The Contracting Officer Representative is notified.

(2) Insider Threat Review Board (ITRB). The MCINCR-MCBQ ITRB is a multidisciplinary team that, when directed by the MCINCR-MCBQ Chief of Staff, will review, investigate, evaluate, and provide recommendations for personnel that have exhibited warning signs and indicators of potential insider threat behavior. Refer to enclosure (1) for ITRB composition.

(3) ITRB Process

(a) Initial report of insider threat behavior is received.

(b) The MCINCR-MCBQ Chief of Staff directs to convene the ITRB.

(c) The CIntP Liaison collects required reports and data, task organizes the ITRB depending on the situation, and assembles the ITRB.

(d) If applicable, the CInTP Liaison will coordinate with the Service Analysis Section, Department of the Navy Analytic Hub. The Service Analysis Section brings together a multi-disciplinary team of professionals with a focus to link disparate pieces of multi-functional information (e.g., counterintelligence, law enforcement, human resources, cybersecurity, etc.) to contextualize anomalous behavior, analyze the data, and identify potential insider threats before they occur. This analysis of gathered information from multiple sources creates a picture of employee activity that may not be available or apparent by reviewing information from only a single source. The Service Analysis Section provides timely notification, referral of information, and mitigation strategies to provide commanders or other decision authorities with a risk decision advantage. The Service Analysis Section of the Department of Navy Analytic Hub can be reached at 703-695-7700, insiderthreat.fct@navy.mil or https://www.secnav.navy.mil/itp/Pages/default.aspx.

(e) When notified by the CInTP Liaison that the ITRB will convene, the Provost Marshal Office provides a summary of the individual's criminal history to the ITRB.

(f) When notified by the CInTP Liaison that the ITRB will convene, Labor and Employee Relations provides a summary of the individual's Official Personnel File to the ITRB.

(g) When notified by the CInTP Liaison that the ITRB will convene, G-6 provides a summary of any questionable activity on the Marine Corps Enterprise Network to the ITRB.

(h) The command representative provides a history of the employee's behavioral concerns, work performance, and any other risk indicators to the ITRB.

(i) Other ITRB members present any pertinent data as applicable.

(j) ITRB reviews all data and generates insider threat mitigation courses of action.

(k) Courses of action reviewed and selected by the MCINCR-MCBQ Chief of Staff.

(4) ITRB Management. The MCINCR-MCBQ Command Security Manager serves as the CInTP Liaison based on the established connection with counterespionage, the Personnel Security Program, and training received at the Marine Corps Security Management Course. The CInTP Liaison is the primary point of contact for the coordination of the ITRB, required documents and reports, and will coordinate with the Service Analysis Section, Department of the Navy Analytic Hub for any reporting requirements or requests for information and support.

c. Tasks

(1) MCINCR-MCBQ Chief of Staff

(a) Refer all reports of insider threat behavior by service members to the appropriate command FPC.

(b) Refer all reports of insider threat behavior by government employees and contractors to the MCINCR-MCBQ ITRB.

(c) Chair the MCINCR-MCBQ ITRB and have final decision authority on insider threat mitigation courses of action.

(2) MCINCR-MCBQ G-3 Operations. Provide the Threat Information Manager to the ITRB.

(3) MCINCR-MCBQ Command Security Manager

(a) Serve as the MCINCR-MCBQ CInTP Liaison.

(b) When directed by the MCINCR-MCBQ Chief of Staff, notify and assemble the ITRB, task organized depending on the situation.

(c) Ensure ITRB members are aware of any report or data requirements for the ITRB. Collects reports and data in preparation for the ITRB.

(d) Coordinate with HQMC or DoN Service Analysis Section for any required reports and analysis.

(e) Manage the MCINCR-MCBQ CInTP Order.

(f) Creates a record of each ITRB in accordance with 5 USC 7114 and ensures proper accessibility and preservation.

(g) Coordinate with NCIS to schedule the Counter Intelligence Brief in order to ensure that all MCBQ personnel receive the training per calendar year.

(4) Commanding Officer, Security Battalion

(a) When requested, provide a National Crime Information Center Criminal History report and Local Records Check for the ITRB.

(b) Provide an organizational representative to the ITRB.

(5) Director, Human Resources and Organizational Management

(a) When requested, provide official personnel files, disciplinary actions, and SF-50s for the ITRB.

(b) Provide a Labor and Employee Relations representative to the ITRB.

(6) MCINCR-MCBQ G-6

(a) When requested, provide information concerning questionable Marine Corps Enterprise Network activity to the ITRB.

(b) When requested, provide an organizational representative to the ITRB.

(7) Commanding Officer, Naval Health Clinic Quantico. When requested, provide subject matter expertise in behavioral / mental health to the ITRB.

(8) Quantico Area Counsel Office. Provide legal guidance regarding labor law, disciplinary or adverse actions, and any developed courses of action for the ITRB.

(9) Naval Criminal Investigative Service, Resident Agency Quantico

(a) Coordinate with the MCINCR-MCBQ Command Security Office to schedule and conduct Counter Intelligence Briefs in order to ensure all MCBQ personnel receive the training per calendar year.

(b) When requested, provide an organizational representative to the ITRB.

(10) Commanders/Directors, Tenant Command and Activities

(a) Establish a CInTP for your respective command or activity.

(b) If the command/activity does not have an established CInTP, refer insider threat behavior of civilian employees and contractors to the MCINCR-MCBQ Chief of Staff or the MCINCR-MCBQ Command Security Manager (assigned as the CInTP Liaison).

(c) Provide a command representative that is knowledgeable of the history of the employee's behavioral concerns, work performance, and any other risk indicators to the ITRB.

5. Administration and Logistics

a. Maintenance. The maintenance of this order belongs to the MCINCR-MCBQ Command Security Manager, who is assigned as the CInTP Liaison.

b. Recommendations. Submit recommendations for changes to the order to the MCINCR-MCBQ Command Security Manager.

c. Privacy Act. 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 shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974") and implemented IAW reference (c).

d. Records Management. Records created as a result of this Order shall be managed according to National Archives and Records Administration (NARA)-approved dispositions per reference (d) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium. Records disposition schedules are located on the Department of Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to reference (d) for Marine Corps records management policy and procedures.

e. Information Management Control. The reporting requirements contained within this Order are exempt from information management control, per National Archives and Records Administration, Transmittal Number 28 (also known as "General Records Schedule 5.6"), Part IV, paragraph 7.o.

6. Command and Signal

a. Command. This order is applicable to all MCINCR-MCBQ elements, commands, and tenants.

b. Signal. This order is effective on the date signed.

MICHAEL L. BROOKS

DISTRIBUTION: A

MCINCR-MCBQ COUNTER INSIDER THREAT PROGRAM (CInTP)

INSTALLATION THREAT REVIEW BOARD (ITRB) CHARTER

1. Forum: Installation Threat Review Board (ITRB).

2. Purpose: The MCINCR-MCBQ ITRB is a multidisciplinary team that will review, investigate, evaluate, and provide recommendations for government employees that have exhibited warning signs and indicators of potential insider threat behavior.

3. Functions.

a. Per MCINCR-MCBQ Order 5510 (Counter Insider Threat Program), the ITRB will convene when directed by the MCINCR-MCBQ Chief of Staff upon receipt of a report of insider threat behavior.

b. The MCINCR-MCBQ Command Security Manager will serve as the Counter Insider Threat Program (CInTP) Liaison based on the established connection with counterespionage, the Personnel Security Program, and training received at the Marine Corps Security Management Course. The CInTP Liaison will be the primary point of contact for the coordination of the ITRB, required documents and reports, and will coordinate with the Service Analysis Section, Department of the Navy Analytic Hub for any reporting requirements or requests for information and support.

c. The ITRB will convene and subject matter experts and command representatives will present pertinent data to assist in the decision making process. The ITRB will develop courses of action (COA) and the MCINCR-MCBQ Chief of Staff will have the final decision authority on the COA.

4. Membership. The ITRB may consist of the following subject matter experts and organizational representatives:

a. MCINCR-MCBQ Chief of Staff (Chairs the ITRB)

b. MCINCR-MCBQ Security Manager (CInTP Liaison)

c. Labor and Employee Relations, Human Resources and Organizational Management

d. Provost Marshal Office

e. Command representative from the employee's organization

f. Medical Officer, Naval Health Clinic Quantico

g. MCINCR-MCBQ Command Inspector

h. Staff Judge Advocate

i. Chaplain

j. NCIS Resident Agency Quantico or NCIS Threat Management Unit

k. MCCS Behavioral Health

l. Sexual Assault Response Coordinator

m. Substance Abuse Counseling Center

n. AFGE Union Representative (if bargaining unit employee)

o. MCINCR-MCBQ Threat Information and Analysis Manager

p. Assistant Chief of Staff, G-6

q. MCINCR-MCBQ Counsel

r. Contracting Officer Representative (if contractor involved)

5. Administration.

a. The ITRB will normally convene in the Commander's Conference Room, 2d deck, Lejeune Hall.

b. The CInTP Liaison will creates a record of each ITRB in accordance with 5 USC 7114 and ensures proper accessibility and preservation.

MCINCR-MCBQ COUNTER INSIDER THREAT PROGRAM (CInTP)

RISK INDICATORS OF POTENTIALLY CONCERNING BEHAVIOR AND ACTIVITIES

1. **Foreign Intelligence Contacts, Activities, Indicators, and Behaviors**

- When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems.
- Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
- Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
- Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
- Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
- Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
- Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities and without explanation.
- Discovery of suspected listening or surveillance devices in classified or secure areas.
- Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
- Discussions of classified information over a non-secure communication device.
- Reading or discussing classified or sensitive information in a location where such activity is not permitted.
- Transmitting or transporting classified information by unsecured or unauthorized means.
- Removing or sending classified or sensitive material out of secured areas without proper authorization.
- Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
- Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
- Improperly removing classification markings from documents or improperly changing classification markings on documents.
- Unwarranted work outside of normal duty hours.
- Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
- Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
- Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.

RISK INDICATORS OF POTENTIALLY CONCERNING BEHAVIOR AND ACTIVITIES

- Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
- Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet.
- Trips to foreign countries that are:
  - Short trips inconsistent with logical vacation travel or not part of official duties.
  - Trips inconsistent with an individual's financial ability and official duties.
- Unexplained or undue affluence:
  - Expensive purchases an individual's income does not logically support.
  - Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture.
  - Sudden reversal of a bad financial situation or repayment of large debts.
- Accepting employment, salary, or any form of payment/compensation or item of value from any foreign government, company, or entity.

2. **International Terrorism Contacts, Activities, Indicators, and Behaviors**

- Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization or expressing sympathy or solidarity with those that do.
- Advocating support or expressing sympathy for a known or suspected international terrorist organizations or objectives.
- Knowingly or intentionally providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
- Procuring supplies and equipment, to include purchasing bomb-making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
- Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
- Expressing an obligation to engage in violence in support of known or suspected international terrorism or expressions of sympathy or solidarity with those that have expressed an obligation to engage in violence in support of known or suspected international terrorism.
- Inciting others to engage in violence in support of known or suspected international terrorism.
- Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
- Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
- Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.

- Repeated browsing or visiting known or suspected international terrorist websites that promote, or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

3. **Foreign Intelligence Entity (FIE) Associated Cyberspace Contacts, Activities, Indicators, and Behaviors**

- Actual or attempted unauthorized access into USG automated information systems and unauthorized transmissions of classified or controlled unclassified information.
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
- Network spillage incidents or information compromise.
- Use of DoD account credentials by unauthorized parties.
- Tampering with or introducing unauthorized elements into information systems.
- Unauthorized downloads or uploads of sensitive data.
- Unauthorized use of USB, removable media, or other transfer devices.
- Downloading or installing non-approved computer applications.
- Unauthorized network access.
- Unauthorized e-mail traffic to foreign destinations.
- Denial of service attacks or suspicious network communications failures.
- Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
- Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
- Data exfiltrated to unauthorized domains.
- Unexplained storage of encrypted data.
- Unexplained user accounts.
- Hacking or cracking activities.
- Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

4. **Workplace Violence Contacts, Activities, Indicators, and Behaviors**

- Direct, indirect, or veiled threats of harm or violence.
- Intimidating, belligerent, harassing, bullying, or aggressive behavior.
- Numerous conflicts with supervisors and other employees.
- Bringing a weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to guns, or unusual fascination with weapons.

RISK INDICATORS OF POTENTIALLY CONCERNING BEHAVIOR AND ACTIVITIES

- Statements indicating the individual is involved in criminal activity.
- 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.
- Statements indicating desperation (over family, financial, and other personal problems) to the point of suicide.
- Pending or recent job layoff.
- Drug/alcohol abuse.
- Extreme changes in behavior, personality, or performance.
- Acquisition of multiple weapons.
- Significant escalation in off-duty, non-work-related target practice or weapons training.
- Menacing actions with weapons.
- Undue interest in explosives.
- Undue interest in previous shootings or mass attacks.
- Conveying a direct or veiled threat of violence to a third party.
- Committing physical assault or wrongful physical violence.
- Engaging in conduct that warrants physical restraint or confinement.
- Stalking or surveillance of individual(s).
- Wrongfully damages or destroys property.
- Blatant or intentional disregard for the safety of others.
- Disruptive, aggressive, or angry language.
- Unusually poor work performance or disciplinary problems at work site.
- Commission of a violent misdemeanor or felony at work site.
- Delusional statements or paranoid ideas.
- Development of a personal grievance.
- Increased isolation.
- Odd or bizarre behavior.
- Loss of personal relationship (e.g., divorce, breakup, family member death).
- Unusual, depressed mood.
- Suicidal ideations.

CInTP NOTIFICATIONS AND REPORTING

Notification of warning signs and behavioral indicators of potential insider threat enables the deterrence, detection, and mitigation process to take place. Notifying the appropriate authority of warning signs and behavioral indicators of potential insider threat is how we take care of our employees. Recognition of the warning signs and behavioral indicators of potential insider threat and notification is foundational to the success of the Program and requires all employees to take this responsibility seriously.

1. Imminent Threat

If there are signs that the insider threat is imminent, an act of violence or crime has already occurred, or if the employee has dire concerns for their safety or the safety of others, contact 911 and PMO/MCPD or the appropriate LE authority immediately.

2. Non-Imminent Threat

If there are NO signs that the insider threat is imminent, the primary means of notification of warning signs and behavioral indicators of potential insider threat shall be through the employee's chain of command or Command Security Manager. If the employee is not comfortable utilizing this approach to report warning signs and behavioral indicators of potential insider threat, the following options are available:

- Report to another Command Security Manager, appropriate level leader or supervisor. This is a reporting option if the person who is displaying warning signs and behavioral indicators of potential violence is in the employee's chain of command or is an immediate supervisor.

- Report directly to the appropriate law enforcement agency (e.g., PMO/MCPD).

- Report directly to the employee's Human Resources Office (HRO).

Notification of insider threat behavior may also be received from the Service Analysis Section, Department of the Navy Analytic Hub. The Service Analysis Section brings together a multi-disciplinary team of professionals with a focus to link disparate pieces of multi-functional information (e.g., counterintelligence, law enforcement, human resources, cybersecurity, etc.) to contextualize anomalous behavior, analyze the data, and identify potential insider threats before they occur. This analysis of gathered information from multiple sources creates a picture of employee activity that may not be available or apparent by reviewing information from only a single source. The Service Analysis Section provides timely notification, referral of information, and mitigation strategies to provide commanders or other decision authorities with a risk decision advantage.

3. NCIS TextTip.

This is a commercial-off-the-shelf (COTS) system purchased and deployed by NCIS to allow anonymous notification. The system allows three methods of notification. All three of these methods encrypt the notifier's data to protect anonymity yet allow NCIS to contact the notifier through an anonymous user alias to gather further information about the report.

- Web-based

Visit https://www.ncis.navy.mil/Resources/NCIS-Tips/ in your web browser.
Click the "Submit a Tip".
Complete the form.

- Text

Text "NCIS" to 274637 from your cell phone.
Receive a response with your assigned anonymous alias.
Begin dialogue.

- Smartphone Application (available for Android and iOS)

Visit App Store and download "NCIS TIPS".
When using for the first time, select a username and password.
When submitting a tip, complete the form and select "Submit".
When you submit a tip using the NCIS Tips mobile app, you can choose to receive push notifications.

4. **EagleEyes (EE)**

EE is the official Marine Corps community awareness Suspicious Activity Reporting (SAR) program. The program is designed to leverage the awareness of community members and non-LE and security personnel to report suspicious activity. The EE program provides the opportunity for anyone to report suspicious activity through the EE website or locally designated phone numbers.

- The EE program educates our Marines, families, civilian Marines, and contractors on typical activities terrorists engage in prior to attack and how to recognize elements of potential terrorist or criminal activities.

- Individuals are encouraged to report suspicious activity through the official website, www.usmceagleeyes.org, providing detailed information and, when possible, imagery from mobile devices, CCTV, security cameras, or other image capturing devices. Individuals can also report by calling the local EE phone number, security personnel, or USMC LE.

- All EE reports submitted via phone call to the local EE phone number, security personnel, or USMC LE shall be entered into the EE system by the security personnel receiving the report.

- All reports submitted through the EE website are automatically uploaded into the Marine Corps Suspicious Activity Information Portal (MCSAIP) and analyzed by designated and specially trained personnel.

- The MCINCR-MCBQ EE phone number is (703) 432-EYES.

5. **Department of the Navy Civilian Employee Assistance Program (DONCEAP)**

DONCEAP provides a comprehensive suite of civilian employee assistance and work/life benefits. Licensed counselors and expert consultants are available 24/7 to help with any personal or work-related concerns.

- https://donceap.foh.psc.gov/

- 1-844-DONCEAP (1-844-366-2327).

- International: 001-866-829-0270.

Local command security managers and local command human resources officers are additional resources.

6. **Marine Corps DSTRESS Line**

The Marine Corps DSTRESS Line provides 24 hours a day, 7 days a week, anonymous phone, chat, and referral service using a "Marine-to-Marine" approach.

- The call center is staffed with veteran Marines, Fleet Marine Force Navy Corpsmen, who were previously attached to the Marine Corps, Marine spouses, and other family members, and licensed behavioral health counselors specifically trained in Marine Corps culture.

- DSTRESS Line's goal is to help callers improve total fitness and develop the necessary skills required to cope with the widely varying challenges of life in the Corps.

- DSTRESS POC includes:

https://usmc-mccs.org/services/support/dstress-line/

Call 1-877-476-7734 to speak anonymously with a live person.

MCINCR CInTP Insider Threat Review Board Process