INTRODUCTION

All DoD Components will report the threshold-level events listed below for covered persons. Covered persons are described in the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System of Records Notice (SORN). ¹

1. The DITMAC mission is to oversee the mitigation of insider threat to DoD personnel, infrastructure, and national security information residing on DoD facilities or networks and to provide DoD Components with an enterprise-level information management capability via the DITMAC System of Systems (DSoS). Key to accomplishing the DITMAC mission in support of the DoD insider threat program is the prompt reporting to the DITMAC following Component processing of insider threat matters meeting one or more of the below DITMAC reporting thresholds.

2. For insider threat matters meeting one or more of the below DITMAC reporting thresholds and for which investigative jurisdiction has been accepted by a Military Department Counterintelligence Organization (MDCO) or by a DoD Law Enforcement Activity (LEA), prompt reporting to the DITMAC will be the responsibility of the MDCO or LEA via the appropriate Component insider threat office. In cases of joint investigations with the FBI, dissemination will be made in accordance with the provisions of the MOU between the FBI and the DoD Governing Information Sharing, Operational Coordination, and Investigative Responsibilities.

3. When, in the opinion of the MDCO or LEA, reporting to the DITMAC would interfere with or potentially compromise criminal or counterintelligence investigations, inquiries, operations, sources or methods, the MDCO or LEA will submit a limited distribution report to the DITMAC via the Component insider threat office. In exceptional circumstances, the first General/Flag Officer or Senior Executive Service official in command or supervision of an MDCO or LEA may determine that limited distribution reporting will not adequately protect a counterintelligence or criminal investigation. Handling of limited distribution reports at the DITMAC will be restricted until such time as the MDCO or LEA informs the DITMAC, via the Component insider threat office, that limited distribution handling is no longer required. The DITMAC will not make any further dissemination of limited distribution reports without the express written permission of the MDCO or LEA exercising jurisdiction over the matter. DITMAC personnel will make no further inquiry efforts on limited distribution reports until such time as the MDCO or LEA informs the DITMAC, via the Component insider threat office, that limited distribution handling is no longer required.

4. DoD Component reporting of threshold-level events to the DITMAC is accomplished via the DSoS, which is accessed on SIPRNet at https://DSoS.DITMAC.smil.mil and by clicking the “Report an Insider Threat” feature.

¹ The following categories of individuals are covered:
   - “Individuals who had or have 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 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.”
   - “Individuals or persons embedded with DoD units operating abroad who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive position.”
   - “Current members of the U.S. Coast Guard and mobilized retired military personnel, when activated, who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive positions by DoD and when operating with the military services or DoD Components, and Limited Access Authorization grantees.”
   - “Individuals who have been issued an active DoD CAC by a DoD Organization to authenticate physical access to DoD installations or logical access to DoD controlled information systems.”
   - “Individuals with an active identification card, pass or credential from a DoD organization used to gain physical or logical access to a DoD facility, network, system or program.”

Notice published at 81 FR 31614 (19 May 16), as altered by notice published at 81 FR 65631 (23 Sep 16), 83 FR 12345 (21 Mar 18), and 84 FR 10803 (22 Mar 19); see also https://www.gpo.gov/fdsys/pkg/FR-2019-03-22/pdf/2019-03540.pdf.
SERIOUS THREAT
Information pertaining to any serious threat covered persons may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. Serious threats are defined as those that present a reasonable risk to life or limb, or have the potential to degrade or destroy a critical intelligence or operational capability of DoD.

ALLEGIANCE TO THE UNITED STATES
Information pertaining to any covered person exhibiting questionable allegiance to the U.S. through words or actions to include involvement in, support of, training to commit, or advocacy of any act, of sabotage, treason, or sedition against the United States.

ESPIONAGE / FOREIGN CONSIDERATIONS
A. The investigation, arrest, or apprehension by a federal law enforcement agency, Military Department Counterintelligence (CI) Organization (MDCC), and/or DoD Component's CI element of any covered person for espionage.
B. Investigations into and/or judicial or administrative actions taken against any covered person regarding reportable Foreign Intelligence Entity (FIE) contacts, activities, indicators, and behaviors as detailed in DoD Directive 5240.06 (Incorporating Change 1, May 30, 2013 “CI Awareness and Reporting” Table 1).
C. Information pertaining to any covered person suspected to have unauthorized contact with an officer or agent of a FIE, or who fails to report or disclose, when required to do so: Any previous or ongoing relationship or contact with any person from a foreign country; foreign travel; foreign passport or identity card; foreign citizenship or foreign residency; foreign military service; ownership of foreign property; or, undue influence by a foreign interest (e.g., on-going personal or professional foreign contacts; receipt of benefits from a foreign country).

PERSONAL CONDUCT
Information, in regard to a covered person, pertaining to deliberate omission, concealment, or falsification of relevant facts from any personnel security investigations, polygraph examinations (including counterintelligence scope and expanded screening scope polygraphs), or a pattern of behavior (two or more incidents closely related in time) that puts the individual's judgment, trustworthiness, candor, honesty, or willingness to comply with applicable laws and regulations into question.

BEHAVIORAL CONSIDERATIONS
Information pertaining to a covered person who exhibits behaviors that cast doubt on their judgment, reliability, or trustworthiness. Such behaviors include, but are not limited to, emotionally unstable, irresponsible, dysfunctional, violent, paranoid, bizarre, anti-social, or aggressive behavior (see "Violence in the Federal Workplace: A Guide for Prevention and Response," referenced below, for additional Information about these behaviors of concern). This also includes information derived from User Activity Monitoring (UAM), human resources information, military and civilian performance evaluations, and reports of criminal or family law proceedings that indicate a person cleared by DoD is a threat to him or herself. Seeking mental health counseling is not by itself a reporting threshold.

CRIMINAL CONDUCT
The investigation, arrest, or apprehension by a federal, state, or local law enforcement agency, or the conviction, indictment, or charging by a federal, state or local jurisdiction of any covered person involving: the loss of life; actual or suspected acts of violence or threats of violence (including sexual assaults); the illegal possession or transfer of weapons of mass destruction; any criminal offenses involving the use of weapons or explosives.

UNAUTHORIZED DISCLOSURE
Information that indicates a covered person is knowingly involved in unauthorized disclosure, theft, loss, or compromise of classified or protected information to a foreign power, an agent of foreign power, the media, or any unauthorized recipient. Reportable unauthorized disclosures include unauthorized publication of classified or controlled unclassified information present in books, articles, or other written, online, or broadcast media sources determined to have been written or otherwise provided by current or former cleared DoD-affiliated officials.

UNEXPLAINED PERSONNEL DISAPPEARANCE
The suspicious death or unexplained disappearance of any covered person.

HANDLING PROTECTED INFORMATION
Information pertaining to a covered person deliberately mishandling protected information, or exhibiting a pattern (two or more incidents closely related in time) of negligent noncompliance with rules, procedures, guidelines, or regulations for protecting classified or controlled unclassified information.

MISUSE OF INFORMATION TECHNOLOGY
Information pertaining to a covered person deliberately misusing information technology, or exhibiting a pattern (two or more incidents closely related in time) of negligent noncompliance with rules, procedures, guidelines or regulations pertaining to information technology.

TERRORISM
Information pertaining to a covered person providing support to, or who is in contact (to include on-line, email, and social networking) with, known or suspected domestic or international terrorist or extremist individuals, organizations, or groups. Any attempt or conspiracy to commit the above shall also be reported.

CRIMINAL AFFILIATIONS
Information pertaining to a covered person providing support to, or who are in contact (to include on-line, email, and social networking) with, known or suspected domestic or international criminal organizations, criminal street gangs, or groups engaged in racketeering activities. Any attempt or conspiracy to conduct the above shall also be reported.

ADVERSE CLEARANCE ACTIONS
The suspension, revocation, or denial of a security clearance of a covered person for reasons identified in thresholds 1-12.