Report Insider Threat Information to the CSA

All suspicious activity, including information gleaned from the Insider Threat Program, is subject to reporting requirements under NISPOM Section 3, paragraphs 1-300 thru 1-302 and Industrial Security Letters (ISL) 2006-02, 2011-04, and 2013-05.

Requirements:

- **Information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines, must be reported when that information constitutes adverse information, in accordance with NISPOM 1-302a and ISLs 2006-02 and 2011-04.**

- **Incidents that constitute suspicious contact must be reported under NISPOM 1-302b and ISL 2006-02**

- **Incidents that constitute information concerning actual, probable or possible espionage, sabotage, terrorism or subversive activities at any of its locations must be reported to the nearest field office of the Federal Bureau of Investigation with a copy to the CSA under NISPOM 1-301, ISL 2006-02, and ISL 2013-05.**

Getting Started:

As part of your facility's overall risk mitigation strategy, the Insider Threat Program is designed to identify indicators, behaviors, and activities associated with potential insider threats and report them appropriately. Events that impact the following ***MUST*** be reported to the Facility Security Officer (FSO), DSS, and in some instances the FBI:

- The status of the facility clearance
- The status of an employee's personnel security clearance
- That indicate an employee poses a potential Insider Threat
- That affect proper safeguarding of classified information
- That indicate classified information has been lost or compromised

Once reported through appropriate channels steps will be taken by responsible parties to analyze the data and take further action. Information reported to DSS may be referred to cognizant security, law enforcement, and intelligence agencies including: Military Department law enforcement, intelligence, and counterintelligence activities; Defense Insider Threat Management Analysis Center (DITMAC); Central Adjudication Facilities (CAFs); and/or local, state, and federal law enforcement as appropriate. Your Insider Threat Program is responsible for identifying and reporting indicators – not prosecuting individuals. It should be noted that mitigating factors often exonerate individuals identified through the program and/or identify security vulnerabilities and appropriate countermeasures.

Best Practices:

- Reporting refers to the transfer of information to the CSA and appropriate authorities. However, it also refers to actions taken by employees to inform the Insider Threat Program of actual or suspected insider threat activities and indicators.

- Ensure that the Insider Threat Program group (program personnel from offices across the contractor's facility based on the organization's size and operations) encourages reporting from personnel and information under their area of responsibility.

- All employees are required to take Insider Threat Awareness training which identifies reportable behaviors and activities. Consider supplementing this annual training with newsletters, job aids, posters and other material to reinforce reporting requirements and responsibilities.

- Work with your DSS Counterintelligence Special Agent, Industrial Security Representative, and Information System Security Professional to identify appropriate response actions including reporting and the development of countermeasures.

Related Training and Resources:

- **eLearning Course: Adverse Information Reporting**
- **eLearning Course: The 13 Adjudicative Guidelines**
- **eLearning Course: Insider Threat Awareness**
- **Insider Threat Toolkit Tab: Reporting**
- **Insider Threat Job Aids/Case Studies**