DEFENSE INTELLIGENCE AGENCY

January 13, 2014

INSIDER THREAT PROGRAM

The insider threat problem set is not new. How we approach the problem set is. Historically, insider threat was viewed solely as a counterintelligence issue. This is not the case. Two seminal events – WikiLeaks and the 5 November 2009 Ft. Hood shooting incident; neither classified as a counterintelligence (CI) matter – changed the basic definition and focus of the insider threat problem set. The new reality -- the Insider Threat Program (InTP) serves as a bridge, leveraging the capabilities of existing programs to capture the synergy of each to deter, detect, defeat, or otherwise mitigate an insider who uses their authorized access, wittingly or unwittingly, to do harm to the security of the United States, to include degradation of departmental resources or capabilities.

Previously, individual disciplines or functions, while focused on the same outcome, were stove piped preventing an effective exchange of information that could aid in the identification of the insider who intends to do harm. Recognizing this, DIA's program was designed as a discipline neutral entity rather than a function of an existing discipline (i.e., CI or Security), nor does the program replace an existing discipline. The program is designed to integrate, synchronize, and leverage existing CI, Security, Information Assurance (IA), Law Enforcement (LE), Human Resources (HR), and other functional capabilities to detect and mitigate the insider threat without prematurely linking the program, or an event, to a specific discipline and thus required to follow the restrictions of policy and law that accompany the individual disciplines. This allows the analysis of a potential insider threat issue to take place, over time if necessary, until an informed decision is made that a threat exists, the facts and circumstances of the threat is within the responsibility of a specific discipline, and the discipline is formally tasked to respond.

The "Hub" of the DIA InTP is the **Threat Mitigation Cell (TMC).** The TMC consists of a small group of professionals with CI, Security, LE, Computer Network Defense (CND), and other experiences necessary to identify anomalous behavior indicative of an insider threat. This team has the broadest of access to employee related data from both the physical and virtual worlds. This group identifies behavior possibly indicative of a potential threat using insider threat detection and analysis and correlation tools, developing a comprehensive picture of the event. As part of this process, TMC analysts and case managers collaborate with the Personnel Security, Polygraph and Investigations Divisions within the Office of Security, and the Counterespionage Division within the Office of Counterintelligence, as well as other entities as necessary to develop a proposed course of action to resolve the matter at hand.

The DIA InTP was intentionally structured with placement of this core process – the gathering and integrating of information for centralized analysis, reporting, and directing the response

capability – is independent of the response disciplines and serves as an "honest broker" in the analysis and response process. The program monitors the response action and if new information warrants, the matter can be redirected to another discipline for resolution. The ability to function across the disciplines bridges the gap when a matter no longer meets the purview of one discipline as responsibility can be transitioned without the loss of momentum.

Ideally, the actions of the responding element will resolve the insider threat matter. Unfortunately, not all threats can be eliminated. To address those that cannot, DIA established the **Insider Threat Mitigation Panel** that serves as the focal point to resolve or otherwise mitigate insider threat related matters that do not lend themselves to a single discipline solution. These include, but are not limited to, insider threat related inquiries and investigations, personnel security matters, and unresolved polygraph examinations. Panel members review the facts and circumstances of an issue and develop a mitigation strategy, which is recommended to DIA leadership for consideration. Once the mitigation strategy is approved, the InTP leverages the appropriate capability, including the TMC, to ensure compliance with the strategy requirements.

A key function of the Panel is to address situations wherein an employee or affiliate is deemed medically or psychologically unsuitable for polygraph testing. Historically, DIA lacked a formal process to address these situations and cases languished for months and even years. The DIA InTP established a formal process addressing suitability determinations, medical and/or psychological validation, and presentation of the case to the Panel, which in turn develops a mitigation strategy to account for the employee's non-suitability for polygraph examination.

Finally, the Panel also serves to validate and develop mitigation strategies in support of the Counterintelligence Risk Assessment process for current and potential employees who are assessed to be critical or high CI risks to the Agency.

DIA's InTP is compliant with key requirements levied by the Executive Branch and Congress, including the National Insider Threat Policy and Minimum Standards signed by the President on 21 November 2012. The Office of the National Counterintelligence Executive (ONCIX) and the National Insider Threat Task Force (NITTF) seniors have recognized DIA's InTP as a barometer for the insider threat community and team members are often sought out to provide assistance to other Executive Branch entities as they establish their own InTPs.

DIA's InTP is the recipient of the 2012 ONCIX award for the best Insider Threat Team in government. DIA's InTP was recognized for excellence in establishing a robust integrated program leveraging the combined capabilities of CI, Security, IA, HR, and other critical mission areas to detect, identify, and respond to the threat posed by the trusted insider. The program captured the synergy of its various elements to deter, defect, defeat, or otherwise mitigate the insider threat and had an active role in the identification and/or resolution of 11 CI and 197 security-related matters, one of which helped to bring about the arrest of a DoD contractor employee for giving national security secrets to a foreign national. The program continues to achieve success and in 2013, DIA's InTP had an active role in the identification and/or resolution of 38 counterintelligence and 182 security-related matters.

Prepared by: Steven D. McIntosh, DIA Insider Threat Program Coordinator, (202) 231-6411