NATIONAL INSIDER THREAT TASK FORCE

MISSION FACT SHEET

Why was the NITTF established?

The National Insider Threat Task Force (NITTF) was established after the WikiLeaks release of thousands of classified documents through the global media and internet. Its mission is to deter, detect, and mitigate actions by employees who may represent a threat to national security by developing a national insider threat program with supporting policy, standards, guidance, and training.

Who runs the task force, and which agencies are involved?

Under Executive Order (E.O.) 13587, the NITTF is co-chaired by the U.S. Attorney General and the Director of National Intelligence. They, in turn, designated the Federal Bureau of Investigation (FBI) and the National Counterintelligence Executive to co-direct the daily activities of the NITTF. The NITTF comprises employees and contractors from a variety of federal departments and agencies (D/A), and its work impacts more than 99 federal D/As that handle classified material. Currently, the following D/As have representatives on the NITTF: FBI, National Counterintelligence and Security Center (NCSC), Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), and Transportation Security Administration. The NITTF responds directly to the Senior Information Sharing and Safeguarding Steering Committee, which was also established under E.O. 13587. The steering committee comprises representatives from largely Intelligence Community agencies with extensive access to classified networks and materials, including the Departments of State, Energy, Justice, Defense, and Homeland Security, CIA, FBI, Office of the Director of National Intelligence, NCSC, National Security Agency, DIA, the Program Manager—Information Sharing Environment, Office of Management and Budget, the National Security Council Staff, and the Information Security Oversight Office.

What is an insider threat?

It is a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource. This threat

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

How does the task force operate?

The NITTF has drawn together expertise from across the government in areas of security, counterintelligence, and information assurance to develop the policies and standards necessary for individual D/As to implement insider threat programs. Part of the NITTF effort involves hosting training and providing D/As with assistance to better educate their workforce to recognize potential insider threat activity, without creating an atmosphere of distrust. The NITTF conducts assessments of the adequacy of insider threat programs within individual D/As. Through its interface with individual D/As, the NITTF identifies and circulates best practices for detecting, deterring and mitigating emerging threats, and continues to assist D/As in troubleshooting issues.

How do you detect an insider threat?

Detection of potentially malicious behavior involves authorized insider threat personnel gathering information from many sources and analyzing that information for clues or behavior of concern. A single indicator may say little; however, if taken together with other indicators, a pattern of concerning behavior may arise that can add up to someone who could pose a threat. It is important to consider relevant information from multiple sources to determine if an employee's behavior deserves closer scrutiny, or whether a matter should be formally brought to the attention of an investigative or administrative entity, such as the FBI or an agency's Inspector General. It is also possible that the individual has no malicious intent, but is in need of help. In either case, the individual may pose a threat to national security, and the situation requires further inquiry.

Do all insider threats involve malicious individuals?

It is critically important to recognize that an individual may have no malicious intent, but is in need of help. We have invested a tremendous amount in our national security workforce and it is in everyone's interest to help someone who may feel he or she has no other option than to commit an egregious act – such as espionage, unauthorized disclosure, suicide, workplace violence, or sabotage. Intervention prior to the act can save an employee's career, save lives, and protect national security information.

There are also unwitting insider who can be exploited by others. Our adversaries have become increasingly sophisticated in targeting U.S. interests, and an individual may be deceived into advancing our adversaries' objectives without knowingly doing so.

Is every agency required to implement the new minimum standards?

Yes, taken together, the E.O. and the national policy mandate that every executive branch agency with access to classified information establish an insider threat program in line with standards and guidance from the NITTF. However, there is a recognition of differing levels of risk—and, therefore, differing levels of protection required—based on such things as size of cleared population, extent of access to classified computer systems, and amount of classified information maintained by the D/A. The national insider threat policy directs heads of D/As to develop their programs using risk management principles. The NITTF is working with D/As, as well as the Classified Information Sharing and Safeguarding Office, to assess the extent of applicability of the minimum standards to each of the 99+ executive branch D/As with access to classified information based on associated risk.

Is this insider threat emphasis going to infringe on anyone's civil rights?

Insider threat programs are developed and operated in coordination with an agency's records management office, legal counsel, and civil liberties and privacy officials to build in protections against infringing upon employees' civil liberties/civil rights, privacy or whistleblower protections. Departments and agencies are required to provide training in these areas to program personnel, as well as the general workforce. Department and agency heads also have a responsibility to ensure these protections are maintained through oversight of their insider threat programs.

Insider threat programs target anomalous behaviors, not individuals. Additionally, government employees who handle classified information understand that, to hold a security clearance, they accept additional oversight of their workplace activities. Employees sign authorizations for the conduct of investigations to obtain and retain security clearances and there are warning banners on computers and in certain areas of facilities that alert people that they have less expectation of privacy.

What harm can someone do to our government based on the unauthorized release of classified information?

When classified information is divulged in an unauthorized manner outside the confines of the U.S. Government national security structure, that information can create situations that are harmful to U.S. interests and, in some cases, could be life-threatening. Classified information in the wrong hands can provide a unique and potentially dangerous advantage to those states and non-state actors whose interests are opposed to those of the United States. For example, the unauthorized release of classified information could: provide details about weapons systems we rely on to defend our country; expose our overseas intelligence operations and personnel; identify critical vulnerabilities in the U.S. national infrastructure which, if exploited, could damage internal U.S. defense, transportation, health, financial, and/or communications capabilities.

How long will the NITTF exist?

The NITTF will be in place until the President determines that the assistance and assessment work of the NITTF has concluded.