
**Joint Statement for the Record**

**The Honorable Francis X. Taylor**
**Under Secretary for Intelligence and Analysis**
**Counterintelligence Executive**
**Senior Information Sharing and Safeguarding Executive**
**U.S. Department of Homeland Security**

**Rear Admiral Steven Andersen**
**Assistant Commandant for Intelligence**
**United States Coast Guard**

**Richard McComb**
**Chief Security Officer**
**U.S. Department of Homeland Security**

**Before the**

**U.S. House of Representatives**
**Committee on Homeland Security**
**Subcommittee on Counterterrorism and Intelligence**

**Regarding**

**"DHS Efforts to Address Counterintelligence and Insider Threat"**

**June 23, 2016**

Chairman King, Ranking Member Higgins, and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department of Homeland Security's (DHS) efforts to address Counterintelligence and Insider Threat. We look forward to providing our joint perspective on the full range of counterintelligence and insider threats we face as a Department.

**Counterintelligence Threat**

DHS continues to face a complex foreign intelligence threat environment. In recent decades, the U.S. Government has made extraordinary strides in adapting to the changing fiscal, technological, and threat environment. However, the challenges of keeping up with the threat have provided opportunities for foreign intelligence entities to expand their scope of collection and operations against the U.S. Government, including at DHS. There also continues to be significant damage done by insiders who engage in unauthorized disclosures.

In the 2016 National Counterintelligence Strategy, President Obama characterized the counterintelligence threat as "daunting" and one that "seeks to undermine our economic strength, steal our most sensitive information, and weaken our defenses." On a daily basis, foreign intelligence entities, including non-traditional actors such as terrorist groups and transnational criminal organizations, use human and technical means, both openly and clandestinely, to steal U.S. national security information that is of vital importance to our security. The interconnectedness of systems and emerging technologies provide our adversaries with novel ways to steal valuable information from the U.S. Government, academic institutions, and businesses – oftentimes from the safety of a computer thousands of miles away. As the cyber-intrusions against the Office of Personnel Management (OPM) illustrated to millions of government employees, federal agencies continue to remain at significant risk of being targeted by foreign adversaries.

Director of National Intelligence (DNI) James Clapper assessed[1] that the leading threat of intelligence collection on U.S. interests is and will continue to be Russia and China, based on their overt intent, capabilities, and broad operational scope. Other state actors in Asia and Latin America pose local and regional counterintelligence threats to U.S. interests. In addition, Iranian and Cuban intelligence and security services continue to view the United States as their top priority for intelligence collection. The DNI further assessed that penetrating and influencing the U.S. national decision-making apparatus and the Intelligence Community (IC) will remain primary objectives for foreign intelligence entities.

[1] James Clapper, Statement for the Record, "Worldwide Threat Assessment of the US Intelligence Community," February 9, 2016, http://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf

International terrorist groups and transnational organized crime organizations continue to operate and strengthen their intelligence capabilities utilizing human, technical, and cyber means. Similar to state actors, these non-state entities successfully recruit human sources and conduct physical and technical surveillance of their targets, with increasing sophistication, in order to evade detection and capture.

Finally, we continue to believe that unauthorized disclosures of sensitive U.S. Government information are and will remain a threat for the foreseeable future. The interconnectedness of information technology systems exacerbates this threat.

**Counterintelligence Strategy and Implementation**

DHS is implementing the National Counterintelligence Strategy of the United States of America 2016. As a result of the broader intelligence transformation that the Office of Intelligence and Analysis has undertaken in the last year, I have made integrating counterintelligence into the broader DHS mission and our Components' worldwide operations one of my top priorities. To emphasize the growing importance of counterintelligence activities, we realigned I&A Counterintelligence Division to directly report to the I&A front office to reflect its Department-wide responsibilities.

We continue to develop a holistic Counterintelligence Program across the Department, leveraging the Homeland Security Intelligence Council to drive integration of counterintelligence activities across the DHS Intelligence Enterprise. Our objectives are to:

- Deepen our understanding of the threats posed by foreign intelligence entities and insider threats to DHS;
- Detect, deter and disrupt these threats through proactive training and awareness campaigns and effective investigative efforts;
- Safeguard sensitive information from exploitation by identifying the department's most critical assets and implementing enhanced protective measures; and
- Support Departmental efforts to protect our Nation's networks from foreign intelligence efforts to disrupt, exploit, or steal sensitive information, including personally identifiable information.

To help coordinate this effort, we created a Counterintelligence and Security Board, co-chaired by the DHS Counterintelligence Director and the DHS Chief Security Officer to better integrate and align Component Counterintelligence and security programs. This Board helps synchronize the Department's counterintelligence efforts, insider threat programs, foreign access and visitor management, and related counterintelligence and security activities.

As part of the effort to integrate counterintelligence into Component missions and operations, I&A Counterintelligence Division is embedding experienced Counterintelligence Officers in each of the Operational Components and highest risk headquarters offices. These Counterintelligence Officers perform myriad functions, including:

- Assisting DHS Component Leadership with their efforts to protect DHS personnel, programs, and information from external and internal threats;
- Conducting comprehensive foreign intelligence threat and awareness briefings, including foreign travel briefings and debriefings for DHS personnel traveling to high threat countries;
- Assisting with periodic Counterintelligence Program Compliance Reviews; and
- Creating a culture of CI awareness through training.

I&A's Counterintelligence Division recently began Departmental counterintelligence capability assessments and program reviews to identify gaps requiring additional resources and prioritize existing resources. The assessments and reviews examine which DHS operations are most vulnerable to foreign intelligence entities, and provide the information necessary to make decisions on defensive counterintelligence operations to counter the foreign intelligence entity threat.

The Counterintelligence Division also produces all-source intelligence analysis of foreign intelligence threats to DHS personnel, operations, technology, and the broader Homeland Security Enterprise, including our State, Local, Tribal, Territorial, and Private Sector partners. I&A recently completed a classified counterintelligence threat assessment covering the last three years. This assessment, which serves as our baseline, will be updated annually to track trends and significant changes in the counterintelligence threat environment.

As a member of the Committee on Foreign Investment in the United States (CFIUS), DHS conducts analysis to support the ODNI-led National Security Threat Assessments. If a National Security Agreement or other risk mitigation agreement is put in place, DHS counterintelligence analysts assess the threat to support DHS CFIUS Compliance Monitoring—the process through which the U.S. Government continuously tracks, evaluates, and enforces CFIUS mitigation measures.

DHS counterintelligence also supports Team Telecom, comprised of the DHS, Department of Justice (DOJ), and Department of Defense (DoD). Team Telecom reviews applications to the Federal Communications Commission (FCC) when there is disclosable foreign ownership and the potential national security, law enforcement, and public interest concerns. Our threat assessment informs Team Telecom's recommendations to the FCC.

We also recognize that much of the DHS workforce and the broader Homeland Security Enterprise does not handle classified information and is not always aware of foreign intelligence entity threats or the relevance of counterintelligence to their work. We work to educate the workforce on their counterintelligence responsibilities.

- In July 2013, I&A's Counterintelligence Division published an unclassified finished intelligence product for our federal, state, and local partners who host foreign delegations and tours on potential indicators of foreign collection techniques. The product highlighted "Topics of Concern" and "Behaviors of Concern" personnel should be aware of that might raise a red flag and encouraged them to report suspicious activity.

- We have also conducted significant outreach following the breach of personnel information from the compromise of OPM databases and the potential threats stemming from that incident to educate the workforce and our stakeholders on how they might be targeted, and encouraged them to report suspicious activity.

To enhance and our counterintelligence program, we are forging strong partnerships within DHS and are partnering with counterintelligence elements across the U.S. Government.

**U.S. Coast Guard Counterintelligence Service**

The U.S. Coast Guard's (USCG) Counterintelligence Service serves as a model for our Components. Established in 2004, the USCG Counterintelligence Service provides defensive counterintelligence support to USCG personnel and units hosting foreign visitors or traveling overseas. Given the USCG's unique maritime mission and frequent international engagements, establishing this capability has proven crucial to protecting USCG personnel from foreign intelligence entity collection attempts and serves as the cornerstone for further development of the Counterintelligence Service's capabilities.

The USCG Counterintelligence Service engages in counterintelligence operations and investigations with partner agencies, and provides its personnel with both online and in-person threat awareness training. The USCG also maintains an internal website that hosts insider threat reference material, as well as a portal employees can use to report insider threat concerns.

The USCG Counterintelligence Service has increased analytic production tailored to the current threat environment, specifically with products related to countering foreign intelligence entities and transnational organized crime collection efforts targeting the USCG.

Most recently, in support of the USCG's Western Hemisphere Strategy and the DHS Southern Borders and Approaches Campaign, the USCG Counterintelligence Service initiated a pilot program to integrate Counterintelligence Service Agents with DoD Force Protection Detachments, supporting the increased USCG presence in foreign countries.

**Insider Threat Program**

With more than 115,000 federal employees who have access to classified national security information, implementing Executive Order (EO) 13587[2] and the President's National Policy and Minimum Standards for Executive Branch Insider Threat Programs is the Department's top information safeguarding priority. Established pursuant to EO 13587, the DHS Insider Threat Program is a department-wide effort to protect classified national security information from unauthorized disclosure. The purpose of the program is to identify, detect, deter, and mitigate the unauthorized disclosure of classified information. The DHS Chief Security Officer serves as the department's Senior Official responsible for the day-to-day management and oversight of the Insider Threat Program.

We have made tremendous strides maturing our program to address insider threats to classified information and we expect to meet the Administration's mandate to make our insider threat program fully operational by the end of the calendar year, including the deployment of monitoring technology on all of our classified computer networks. This includes the Secret-level Homeland Secure Data Network, which provides classified connectivity to our 23 federal agency subscribers and nearly all State and Local Fusion Centers.

Significantly, the USCG became the first Insider Threat Program in the Executive Branch to achieve "Full Operating Capability" status as assessed by the National Insider Threat Task Force. USCG has been addressing insider threats since 2008, and, in 2012, installed technologies designed to assist in addressing insider threats on classified computer systems. USCG's technical detection capability – staffed by engineers and analysts – spans all classified USCG computers, fuses information from other organizations, and has constant oversight.

In addition to the deployment of monitoring technology to all of our classified networks, we have implemented the capability to collect, fuse, correlate, and analyze information from various data sources in order to identify suspected insider threats. This capability has constant oversight by our General Counsel, Privacy Officer, and Officer for Civil Rights and Civil Liberties in order to ensure the protection of privacy, civil rights, and civil liberties of all of our personnel.

[2] EO 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

We strongly believe that in order to prevent insider threats from materializing through early intervention, we must educate and train our workforce to "See Something, Say Something." We are in the process of providing our workforce with comprehensive awareness training to better sensitize our workforce to identify and report anomalous behavior indicative of an insider threat. This training, which will serve as a force multiplier for our program, enables the detection of potential threats that cannot be discovered through any technological solution available today. Earlier detection will allow for earlier mitigation of potential threats and we believe this is a key component of our program.

The Insider Threat Program complements the Department's counterintelligence and security missions. In recognition of this, the Department is currently considering expanding the scope of our program to include preventing, deterring, detecting, and mitigating other threats posed by insiders such as workplace violence, criminal activity, and misconduct.

**Conclusion**

Chairman King, Ranking Member Higgins, and Members of the Committee, we thank you again for the opportunity to appear before you today to discuss these important matters. We look forward to answering your questions.