COUNTERINTELLIGENCE AND INSIDER THREATS: HOW PREPARED IS THE DEPARTMENT OF HOMELAND SECURITY?

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 13, 2016

Serial No. 114–82

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE

24–382 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PETER T. KING, New York, *Chairman*

CANDICE S. MILLER, Michigan
LOU BARLETTA, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MICHAEL T. MCCAUL, Texas *(ex officio)*
BRIAN HIGGINS, New York
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MANDY BOWERS, *Subcommittee Staff Director*
JOHN L. DICKHAUS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Staff Director*

CONTENTS

COUNTERINTELLIGENCE AND INSIDER THREATS: HOW PREPARED IS THE DEPARTMENT OF HOMELAND SECURITY?

Wednesday, July 13, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Peter T. King (Chairman of the subcommittee) presiding.

Present: Representatives King, Katko, Hurd, Higgins, and Vela.

Also present: Representative Jackson Lee.

Mr. KING. Good morning. The Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will come to order. The subcommittee is meeting today to hear testimony from the Department of Homeland Security regarding counterintelligence and insider threat programs.

I would like to welcome my good friend, Mr. Higgins, Ranking Member of the subcommittee, and express my appreciation to the witnesses who are here today on this vital topic. I also want to express my appreciation for your flexibility. As you know, we had to postpone this meeting from its previously scheduled date, and I really appreciate you accommodating our schedule. So thank you very much.

At the outset of today's hearing, I want to stress that the subject matter is sensitive, and after consultation with the Ranking Member and the Department, I will move to close the hearing at some point after the public statements and some initial questions. We will reconvene in a Classified setting to continue the hearing. To that end, if other Members arrive before we move the hearing, I would ask them to consider their questions and reserve any that are sensitive for the closed portion.

Today we find our Nation confronting a complex external threat picture that ranges from ISIS, al-Qaeda and its affiliates, to traditional foes, such as Russia, Iran, and China. Earlier this year, General Clapper, the Director of National Intelligence, said, "Unpredictable instability has become the new normal and this trend will continue for the foreseeable future."

Compounding this danger, there have been a series of appalling events over recent years involving trusted individuals working inside our Government who damaged National security or committed tragic acts of violence.

Foreign intelligence services and transnational criminal organizations dedicate years of time and financial resources to develop an asset with the access that an insider like Bradley Manning, Edward Snowden, Aldrich Ames, and Robert Hanssen possessed.

Information illegally released by WikiLeaks and Snowden's treacherous acts highlight the link between counterintelligence and the need to spot insider threats before they cause grave risk to National security and put lives at risk.

The Department of Homeland Security has recently experienced a number of troubling cases where trusted insiders have carried out violent acts or have been arrested for having unauthorized weapons at work. A DHS employee was arrested in early June when he was found carrying a gun inside DHS headquarters. I know the case is on-going and the individual's intent is not known, but the case does raise serious questions. The public court documents definitely raise concerns that he may have intended to, "commit an act of workplace violence."

Yesterday, there was another case at DHS headquarters where a contractor was discovered with a gun. If reports are accurate, this is the second case in a little over a month of employees discovered through random checks with weapons. I know the witnesses will agree, this requires immediate attention by the Department to protect its work force.

In May, an officer with the Federal Protective Service system murdered his wife and several other people.

The subcommittee is holding this hearing to review DHS's counterintel and insider threat programs. With over 100,000 employees holding security clearances and significant responsibilities for the country's border, cyber, and maritime security, DHS represents a prime target for the intelligence collection efforts of our enemies.

Unauthorized disclosures of Classified information, whether deliberate or unwitting, represent a significant threat to National security, the very nature of modern communications and the reliance on electronic data storage and transfer, as well as DHS's information-sharing leadership role with State, local, and Tribal partners, adds complexity to the challenge and requires thoughtful programs to educate employees to mitigate the threat.

The subcommittee wants to hear how the Department is developing robust and holistic counterintelligence and insider threat programs to defend against threats both virtual and physical. We also seek to examine the partnership DHS has developed within the agency and across the Government to leverage best practices. We must determine what actions the Department can take to prevent these threats by proactively identifying and intervening when necessary, to protect DHS, its work force, and the country.

I want to thank our distinguished panel for being here today. Your input is very valuable in showing the benefits of strong counterintel and insider threat programs extend beyond DHS, but to the work force as well, by preserving security and safety and allowing DHS to fulfill its vital homeland security mission.

[The statement of Chairman King follows:]

STATEMENT OF CHAIRMAN PETER T. KING

JULY 13, 2016

Today we find our Nation confronting a complex external threat picture that ranges from ISIS, al-Qaeda and its affiliates, to traditional foes such as Russia, Iran, and China. Earlier this year, the Director of National Intelligence said, "unpredictable instability has become the new normal and this trend will continue for the foreseeable future."[1]

Compounding this danger, there have been a series of appalling events over recent years involving trusted individuals working inside our Government who damaged National security or committed tragic acts of violence.

Foreign intelligence services and transnational criminal organizations dedicate years of time and financial resources to develop an asset with the access that an insider like Bradley Manning, Edward Snowden, Aldrich Ames, and Robert Hanssen possessed.

Information illegally released by Wikileaks and Snowden's treacherous acts highlight the link between counterintelligence and the need to spot insider threats before they cause grave damage to National security and put lives at risk.

The Department of Homeland Security has recently experienced a number of troubling cases where trusted insiders have carried out violent acts or have been arrested for having unauthorized weapons at work.

- A DHS employee was arrested in early June when he was found carrying a gun inside DHS Headquarters. I understand that the case is on-going and the individual's intent is not yet known but the case does raise serious concerns. The public court documents definitely raise concerns that he may have intended "to commit an act of workplace violence."[2]
- Yesterday there was another alarming case at DHS headquarters where a contractor was discovered with a gun. If reports are accurate, this is the second case in a little over a month of employees discovered through random checks with weapons. I know that the witnesses will agree that this requires immediate attention by the Department to protect its workforce.
- In May, Eulalio Tordil, an officer with the Federal Protective Service (FPS), murdered his wife and several other people.

The subcommittee is holding this hearing to review DHS's counterintelligence and insider threat programs. With over 100,000 employees holding security clearances and significant responsibilities for the country's border, cyber, and maritime security, DHS represents a prime target for the intelligence collection efforts of our enemies.

Unauthorized disclosures of Classified information, whether deliberate or unwitting, represent a significant threat to National security. The very nature of modern communications and the reliance on electronic data storage and transfer, as well as DHS's information-sharing leadership role with State, local, and Tribal partners, adds complexity to the challenge and requires thoughtful programs to educate employees to mitigate the threat.

The subcommittee wants to hear how the Department is developing robust and holistic counterintelligence and insider threat programs to defend against threats both virtual and physical. We also seek to examine the partnerships DHS has developed within the agency and across the Government to leverage best practices. We must determine what actions the Department can take to prevent these threats by proactively identifying and intervening when necessary to protect the DHS, its workforce, and the country.

I would like to welcome our distinguished panel. Your input today is very valuable in showing that the benefits of strong counterintelligence and insider threat programs extend beyond the DHS enterprise, but to the workforce as well, by preserving safety and security, and allowing DHS to fulfill its critically important homeland security mission.

Mr. KING. With that, I recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Higgins.

---

[1] Director of National Intelligence (DNI) James Clapper, testifying before the Senate Armed Services Committee, 2016 Worldwide Threats Hearing, February 9, 2016, official DNI Twitter account, available at: *https://twitter.com/odnigov/status/697145988406972420*.

[2] Scott McFarlane, "Feds Investigating Whether Employee was Plotting Attack on Homeland Security Officials", NBC News Washington, June 21, 2016, available at: *http://www.nbcwashington.com/investigations/Feds-Investigating-Whether-Employee-Was-Plotting-Attack-on-Homeland-Security-Officals-383852591.html*.

Mr. HIGGINS. Thank you, Mr. Chairman.

I would like to thank Chairman King for holding this hearing. I would also like to thank the witnesses for participating in today's hearing.

Many of the issues that come before this committee are and have been mainstays in the public discourse since the terrorist attacks of September 11. However, the security clearance process and protection of our Classified networks and information arguably did not become permanently affixed to our National and international security conversations until May 2013. That is when we learned that former NSA contractor Edward Snowden leaked the details of Classified programs to the British newspaper *The Guardian.*

The sheer volume of the information shared by Snowden brought many issues to the forefront of our National security conversations. Since the leak, Congress and the public have questioned if an outside contractor should have vetted his security clearance or it was a duty that should have rested squarely with the hands of the Federal employees. We have questioned if Snowden should have had access to such sensitive information in massive volumes.

Then, later that same year, we learned that the same firm that vetted Edward Snowden also vetted the Navy Yard shooter Aaron Alexis. On September 16, 2013, Alexis, a civilian contractor, opened fire at the Navy Yard here in Washington, DC—literally, within walking distance of where we sit today. In the subsequent investigation, we learned that Alexis failed to disclose information about felony charges and a Federal personnel report had no information about his previous arrests.

In May of this year, a Federal Protection Services employee, Officer Tordil, who had held a TS and SCI clearance since November 2015, shot and killed his estranged wife outside a high school in Maryland, then later killed two more people outside a mall and grocery store in Maryland.

All of these incidences have raised concerns that we will discuss today. Had a strong insider threat program been in place, NSA authorities would have been alerted to massive amounts of information being transferred by Snowden for public distribution. Continuous evaluations of Aaron Alexis may have flagged his arrest and felony charges.

While I understand the limitations of insider threat and counterintelligence programs, I also see the value in having such programs today. I also look forward to expanding the conversation to consider the role right to privacy plays in these programs in securing the country. Finding this balance is difficult, but today I hope to learn what the Department of Homeland Security is doing to advance their insider threat and counterintelligence programs. I look forward to the robust discussion with our witnesses today.

I yield back.

[The statement of Ranking Member Higgins follows:]

STATEMENT OF RANKING MEMBER BRIAN HIGGINS

JULY 13, 2016

Many of the issues that come before this committee are and have been mainstays in the public discourse since the terrorist attacks of September 11. However, the security clearance process and protection of our Classified networks and information,

arguably, did not become permanently affixed to our National and international security conversations until May 2013.

That is when we learned that former NSA contractor Edward Snowden leaked the details of Classified programs to the British newspaper *The Guardian.* The sheer volume of information shared by Snowden brought many issues to the forefront of our security conversations.

Since the leak, Congress and the public have questioned if an outside contractor should have vetted his security clearance or if it was a duty that should have rested squarely in the hands of Federal employees. We have questioned if Snowden should have had access to such sensitive information in massive volumes.

Then, later that same year, we learned the same firm that vetted Edward Snowden also vetted the Navy Yard shooter, Aaron Alexis. On September 16, 2013, Alexis, a civilian contractor, opened fire at Navy Yard here in Washington, DC, literally within walking distance of where we sit today. In the subsequent investigation we learned that Alexis failed to disclose information about felony charges and a Federal personnel report had no information about his previous arrests.

In May of this year, Federal Protective Services employee Officer Tordil, who had held a TS/SCI clearance since November 2015, shot and killed his estranged wife outside of a high school in Maryland. Then, later killed two more people outside a mall and grocery store in Maryland. All of these instances have raised concerns that we will discuss today.

Had a strong Insider Threat program been in place, NSA authorities would have been alerted to massive amount of information being transferred by Snowden for public distribution. Continuous evaluations of Aaron Alexis may have flagged his arrests and felony charges.

While I understand the limitations of Insider Threat and Counterintelligence programs, I also see the value in having such programs. Today, I also look forward to expanding the conversation to consider the role "the right to privacy" plays in these programs and securing the country.

Finding this balance is difficult, but today I hope to learn what the Department of Homeland Security is doing to advance their Insider Threat and Counterintelligence programs.

Mr. KING. I thank the Ranking Member. Any other Members of the subcommittee, whether here or not, may submit statements for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 13, 2016

In a time where threats and issues regarding domestic and foreign terrorists, emergency preparedness, immigration, and aviation seem to be at the forefront of our thoughts and concerns, the issues surrounding how we secure the information that informs all of those polices is often forgotten.

In the nearly decade and half since the 9/11 attacks, both the committee and security officials have worked together to increase the security workforce and information needed to better secure our homeland.

One of the primary recommendations from the 9/11 Commissioners encouraged the United States to improve its intelligence gathering and information-sharing activities.

This resulted in more employment positions that allow access to Classified information, which requires security clearances.

While it is clear that the sharing of Classified and Unclassified information between our domestic and international partners is imperative to keep us all safe, it also presents a number of issues.

Of those issues, the one we will discuss at length today is the increase in opportunities for bad actors to exploit our workforce and information through sabotage, theft, espionage, and fraud. Bad actors commit these acts in order to gain competitive advantages for economic and political reasons all over the world.

Another issue is the massive proliferation of original and duplicative Classified material and the exponential growth in the number of individuals with security clearances.

Both present significant homeland and international security challenges.

An estimated 4.5 million people held security clearances in fiscal year 2014.

The costs of security clearance investigations vary significantly, depending on clearance levels.

However, in fiscal year 2014 the minimum cost for a Top-secret clearance investigation was almost $4,000, while the minimum cost of a Secret clearance was $3,000.

Additionally, the cost of maintaining the security classification system across the Federal Government was estimated at more than $11 billion for fiscal year 2013.

Within that amount, the estimate for the cost of protecting and maintaining Federal Classified information was more than $4 billion.

To say we have made a significant financial investment in our Classified security systems is an understatement.

However, none of those financial resources matter as much as the continued investment that needs to be made to monitor those systems.

In order to address the continuing increase of Classified information, positions, and systems needed to protect Classified data, I will reintroduce legislation titled the "Clearance and Over-Classification Reform and Reduction Act" or "CORRECT Act."

While the CORRECT Act addresses Government-wide security clearance processes, in order to advance more focused legislation, I also introduced H.R. 3505, "Department of Homeland Security Clearance Management and Administration Act."

This act makes specific classification reforms within the Department of Homeland Security.

Subsequently, that bill has passed our committee and the House with bipartisan support.

If enacted, H.R. 3505 would make DHS a leader among Federal agencies with respect to security clearance and position designations practices.

I believe that access to National security information is a privilege that should be regarded with the highest integrity and it is important for the Department to be good stewards of this information by managing and monitoring its workforce and data.

I look forward to hearing from our witnesses today regarding the best practices and considerations undertaken to further the programs directed at counterintelligence and insider threats to the Department of Homeland Security and its personnel.

Mr. KING. We are pleased to have a very distinguished panel of witnesses before us today on this vital topic. All the witnesses are reminded, their written testimony will be submitted for the record.

We will hear first from Under Secretary Frank Taylor. The Honorable Frank Taylor has served as the under secretary for intelligence and analysis and as the chief intelligence officer for the Department since April 2014.

Prior to joining DHS, Secretary Taylor served with great distinction in the U.S. military for 31 years, rising to the rank of brigadier general. He has also served in numerous senior positions in the State Department, focused on counterterrorism and security of U.S. personnel, and he has also worked in the private sector.

Most importantly, of course, he holds a bachelor's and master's degree from the University of Notre Dame. Go Irish.

I now recognize General Taylor.

STATEMENT OF HONORABLE FRANCIS X. TAYLOR, UNDER SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY

General TAYLOR. Thank you, Chairman King, Ranking Member Higgins. I would start with "Go Irish" given our shared lineage with the University of Notre Dame. I want to thank you and the Members of the committee for the opportunity to appear with my colleagues here today.

The Department faces a range of threats from foreign intelligence services, non-state entities like terrorist groups and transnational criminal organizations, and insider threats. Based on overt intent, capabilities, and broad operational scope, Russia and

China continue to be the leading state intelligence threats to the United States and our interests, including the Department of Homeland Security.

Similar to foreign intelligence threats, terrorist groups and TCOs continue to enhance their human, technical, and cyber intelligence capabilities recruiting human sources and conducting physical and technical surveillance of DHS operations. Additionally, we are very concerned that the threat from insiders disclosing sensitive U.S. Government information will also continue.

As the Department's counterintelligence executive, I am leading the implementation of the new National Counterintelligence Strategy and building out a unified Department counterintelligence program. I am also the Department's senior information-sharing and safeguarding executive responsible for overseeing all Classified information-safeguarding efforts in our Department.

We recently completed a Classified assessment of foreign intelligence threats to the Department and the broader homeland security enterprise. This will serve as our baseline assessment, and we will re-evaluate this assessment every year to track trends and update it with significant changes in the CI threat environment.

Thanks to Congress, Congressional support, we have significantly enhanced our counterintelligence and threat programs. I&A's Counterintelligence Division has Department-wide responsibilities. Our objectives are to deepen our understanding of the external and internal threats; deter, detect, and disrupt these threats; safeguard sensitive information from exploitation; and to protect our Nation's networks from foreign intelligence threats, such as the disruption, exploitation, or theft of sensitive information, including personally identifiable information.

We are embedding counterintelligence officers in each of the Department's operational components and within the Department's most at-risk headquarters components. We are also leveraging the existing resources, like the U.S. Coast Guard Counterintelligence Service, and are partnering with CI personnel from across the Federal Government to enhance the Department's CI program.

These are just a few of the steps we are taking to meet these threats so the Department can continue its work securing the country and fulfilling our border security, immigration, travel security, and other homeland security missions.

Our Insider Threat Program has made great progress implementing Executive Order 13587. For this fiscal year, our technical monitoring solution audited 33 million actions on our enterprise Classified networks. Of these, 215,000 required manual review by our analysts, of which 72 required further investigation. During the previous 2 fiscal years, the Insider Threat Program also identified 162 violations and provided support to 15 counterintelligence and internal security investigations.

Chairman King, Ranking Member Higgins, Members of the committee, thank you again for the opportunity to appear before you to have this very important discussion. I look forward to your questions.

[The joint prepared statement of General Taylor, Colonel McComb, and Rdml. Andersen* follows:]

JOINT PREPARED STATEMENT OF FRANCIS X. TAYLOR, RICHARD MCCOMB, AND STEVEN ANDERSEN

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.

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' world-wide operations one of my top priorities. To emphasize the growing importance of counterintelligence activities, we realigned I&A Counterintelligence Divi-

* Rdml. Robert P. Hayes, Assistant Commandant for Intelligence, U.S. Coast Guard, U.S. Department of Homeland Security testified on behalf of Rdml. Andersen.

[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*.

sion 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 3 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

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

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.

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.

Mr. KING. Thank you, General. Thank you really for the outstanding job you have done and the dedication you have shown to this job. It is very much appreciated.

Colonel McComb was appointed to the position of chief security officer for the U.S. Department of Homeland Security just over 3 months ago, on April 3, 2016. Most recently, he served as the director of the Leased Facilities Protection Directorate at the Pentagon Force Protection Agency. Colonel McComb served over 27 years in the United States Air Force as a security forces officer, from which he retired as a colonel.

We are privileged to have you here today, and you are recognized for your testimony.

STATEMENT OF RICHARD D. MC COMB, CHIEF SECURITY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Colonel MCCOMB. Chairman King, Ranking Member Higgins, good morning, and thank you for the opportunity to provide Department of Homeland Security's Insider Threat Program.

I have the opportunity to lead the dedicated men and women who make up the Office of Chief Security Officer. My office is an element under the Department's Management Directorate and I report to the under secretary for management, Mr. Russ Deyo.

However, in my capacity as a senior insider threat official for the Department of Homeland Security, under the provisions of Executive Order 13587, I execute the Insider Threat Program on behalf of and under the guidance and direction of Under Secretary Frank Taylor, as the under secretary for intelligence and analysis.

As a chief security officer, I am responsible for DHS-wide related programs affecting more than the 235,000 employees that make up the Department, including the areas of personal security, physical security, investigations, administrative security, identity management, special access programs, security training awareness, and the Department's Insider Threat Program.

Finally, I serve as the chairman for the Department's Chief Security Officer Council and have an opportunity to lead, with my other counterparts in the DHS components, a highly collaborative secu-

rity program that is designed to safeguard the Department's people, property, and information.

The DHS Insider Threat Program seeks to deter, detect, and mitigate threats posed by trusted insiders. The program uses technology that is generally called user activity monitoring. This technology puts effective capability behind the warning banners which for years have told users they were being subject to such monitoring. The detection thresholds are tailorable to specific types of users and to specific types of behaviors.

This is important, that for the first time the activity of tens of thousands of users on IT systems can actually be monitored via automation and, when combined with information from other data sources, present a total threat picture. When automated analysis is added in, the software can alert analysts to events that have a high threat potential and minimize wasteful false positives.

While this technology is a critical facet of our program, it also relies on aggressive training and awareness for the work force to enable and empower them to recognize aberrant behavior and to include the tools to responsibly report it when they see something.

I want to emphasize that the Insider Threat Program is part of the security continuum, one of the elements in a series of steps and programs to mitigate the full spectrum of risks posed by employees, contractors, and other officials affiliated with the DHS, as well as external actors who may threaten the Department from outside.

As presently structured, our Insider Threat Program focuses on the protection of Classified information as it was originally driven by the Manning and Snowden cases. However, DHS, as well as DOD and the intelligence community, are taking a more expansive view of the threat to include workplace violence, fraud, waste and abuse, and other potential work force corruption.

The Office of the Chief Security Officer and the authorities exercised by it uniquely situate the organization to execute this program, connect the necessary dots, and detect and prevent such threats.

DHS is currently monitoring 2 or 3 IT systems. We are in the process of ensuring that our insider threat training awareness program meets 508 compliance to ensure accessibility by those with disabilities. Once completed, this training will be posted on our Performance and Learning Management System to enable the work force to meet the initial and annual training requirements.

As was indicated earlier, resources are key to the maturation of this program. Currently, we are learning what we can expect to discover on Classified systems, but Unclassified systems will present much broader risk, with far more users, and will require greater analysis and follow-on investigative capabilities. We have programmed for funding and support of this expansion consistent with the current proposed insider threat legislation.

In conclusion, access control to Federal facilities, information by Federal employees and contractors, and a safe, secure workplace are Departmental priorities and one in which the Office of the Chief Security Officer has made significant progress. However, there is more work to be done, and the Office of the Chief Security Officer, in coordination with the under secretary for intelligence

and analysis and the DHS components, has charted a clear course to further mitigate the concern of the insider threat.

Thank you again for the opportunity to testify today, and I look forward to your questions, sir.

Mr. KING. Colonel, thank you.

Our next witness is Rear Admiral Robert Hayes, who just recently took on the mantle for Coast Guard intelligence activities, assuming the post of assistant commandant for intelligence just earlier this month. Prior to this command, Admiral Hayes served as chief of plans and policy for the assistant commandant for intelligence and criminal investigations. Prior to that, served as deputy director of the Coast Guard's Counterintelligence Service.

He graduated from the Coast Guard Academy in 1988 and earned a master's in strategic intelligence with the National Intelligence University in 1993.

Admiral Hayes, good to have you here today. I look forward to your testimony. Thank you.

STATEMENT OF ROBERT P. HAYES, ASSISTANT COMMANDANT FOR INTELLIGENCE, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral HAYES. Thank you, Chairman King. Good morning, sir. Good morning, Ranking Member Higgins and other distinguished Members of the committee.

I am honored to be here today to discuss the Coast Guard's counterintelligence and insider threat programs. It is a pleasure to be alongside my Department of Homeland Security colleagues, Under Secretary Taylor and Chief Security Officer McComb. I echo Under Secretary Taylor's assessment of the range of intelligence collection threats that face the Department and the Coast Guard.

As the world's premier multimission maritime service responsible for the safety, security, and stewardship of the Nation's waters, the Coast Guard offers a unique and enduring value proposition to the Department of Homeland Security and the American public. At all times a military service and branch of the Armed Forces, a Federal law enforcement agency, a regulatory body, a first responder, and a member of the U.S. intelligence community, the Coast Guard is under high demand as a global instrument of National security.

One of the key elements of the Coast Guard's intelligence enterprise is our counterintelligence program. In 2004, the Coast Guard began the initial development of its counterintelligence capability. In the early stages of development, counterintelligence activities were primarily defensive in nature, providing support to Coast Guard personnel in units either hosting foreign visitors or traveling overseas.

Given the Coast Guard's extensive international engagement with maritime stakeholders, establishing counterintelligence capability was crucial to protecting Coast Guard personnel from foreign intelligence collection attempts and served as the cornerstone for further development of other counterintelligence activities.

Today, the Coast Guard's Counterintelligence Service protects our work force through detection, deterrence, and neutralization of foreign intelligence threats by leveraging authorities and capabilities to provide the full spectrum of counterintelligence support. We

do this through many activities, including counterintelligence investigations, operations, collections, and analysis. These activities shield Coast Guard operations, personnel, systems, facilities, and information from the intelligence activities of not only foreign powers, but terrorist groups and criminal organizations, as Under Secretary Taylor mentioned.

In addition to the counterintelligence mission, the Counterintelligence Service manages and executes the Coast Guard's Insider Threat Program, which began formally addressing insider threats in 2008. In 2012, the Coast Guard officially chartered an Insider Threat Working Group. The Counterintelligence Service staffed a small team to address insider threat requirements and began installation of activity-monitoring technologies designed to detect insider threats on Classified computer systems.

Additionally, the director of the Coast Guard Counterintelligence Service was appointed as the senior official for the Coast Guard Insider Threat Program. A National Insider Threat Task Force assessment of the Coast Guard's Insider Threat Program resulted in the Coast Guard becoming the first insider threat program in the Executive branch to achieve full operating capability earlier this year. The National Insider Threat Task Force also refers to the Coast Guard's Insider Threat Program as the gold standard for small organizations.

The Coast Guard's Insider Threat Program has transitioned from seeking help from partner agencies to providing it. We have advised the Department of Defense on the conduct of technical insider threat detection on Classified computer systems at sea; we have compared and contrasted best practices with other departments; and we have provided best practices to Executive branch agencies, as well as some combatant commands.

Our technical detection capability, which is staffed by engineers and analysts, spans all Classified Coast Guard computer systems in its continuous oversight from Coast Guard leadership and legal counsel. Since inception, we have identified or supported the detection of multiple threats. The overwhelming majority of these detections have been non-malicious types of unauthorized disclosures, password sharing, and system administrator privilege abuse. Despite the absence of harmful attacks, we must remain vigilant by continuing to mature the insider threat and counterintelligence program.

Thank you for inviting me to discuss the Coast Guard's counterintelligence and insider threat programs, and I look forward to your questions, sir.

Mr. KING. Thank you, Admiral.

I will keep my questions brief prior to the closed session.

Colonel McComb, there have been two very public cases of employees arrested with guns at work in the last month that I mentioned in my opening statement. What is your overall assessment of security at the DHS facilities and your ability to identify insider threats that could pose a physical threat?

Colonel MCCOMB. Thank you, sir.

As you may or may not know, the DHS headquarters is a level 5 facility; that is, we meet the standards of the Interagency Security Committee, which is the highest level with regard to Federal

facilities. We meet those standards at the DHS headquarters in the Nebraska Avenue complex, and we are implementing enhanced security measures which are above and beyond the basic measures required by those standards.

As you alluded to, during those enhanced security measures, which includes random screening of employees, we did detect individuals that were attempting to bring unauthorized items into the DHS headquarters. They are currently under investigation, but in both instances we have not detected anything that would lead us to believe that these individuals were planning any sort of workplace violence or conspiring with others to commit workplace violence.

We take security very seriously. I think we do a great job, and I believe our enhanced security measures worked in these cases.

In addition to the enhanced security measures that are being employed at this location, we have taken on a large employee education effort, which includes townhall meetings, communications to the employees to understand that if they see something unusual to report it, and including training to include insider threat training and also emergency management training for how to respond in certain cases.

So the Department is very committed to ensuring that folks are protected within our headquarters, and the DHS complex at Nebraska Avenue complex is no exception to that rule, sir.

Mr. KING. Thank you.

I guess I will ask this across the board. Is there a renewed sense of urgency in the Department and the administration to expedite the implementation of continuous evaluation programs in the wake of the OPM breach?

Colonel MCCOMB. Sir, the DNI, the Director of National Intelligence, has the lead for the continuous evaluation. As you may or may not know, that program will be automated. It is yet to happen, but when it does, there will be 7 authoritative databases that individuals that have National security determinations or possess Secret or above clearances will be vetted against those either on a daily basis or monthly basis, dependent upon the particular data base.

If an individual indicates a hit from one of those databases, then the Department of Homeland Security, along with all of the other departments that participate in this program, will be required to follow that lead, vet that individual, and determine whether it has implication on their ability to perform their job and/or have access to National security information.

There is a time line that 5 percent of the tier 5, that is, those with TS/SCI clearances, must be in a continuous evaluation program by September 2017. We in DHS have already initiated the work to ensure that our IT systems allow us to receive those alerts from the DNI automated program. We will do a pilot program this year to start doing some of those continuous evaluations on our, once again, most sensitive population, those with TS/SCI clearances.

Mr. KING. OK. Anybody else want to comment on that? OK, thank you.

Ranking Member Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Taylor, I just want to continue this line of questioning on the issue of Homeland Security headquarters. For the second time in a month, an employee has been arrested for taking a handgun onto the secured grounds of the Department of Homeland Security at their headquarters here in Washington, DC. According to police records, the accused had a 9-millimeter handgun in a leather handbag while inside the complex. The accused is a contractor who works in the information technology for the agency. The weapon appeared to be fully functional, capable of being fired by a single hand, and designed to expel a projectile by the action of an explosive.

This arrest comes about a month after the arrest of another individual, another Homeland Security employee accused of carrying a firearm inside agency headquarters. Court filings from the investigators indicated that the accused, the second individual, was found with a loaded .22-caliber handgun carrying 5 hollow-point bullets in June.

In that same court filing, it said that the agent was, "probable cause to believe that the accused was conspiring with another to commit work force violence, and more particularly, may have been conspiring or planning to commit violence against a senior DHS official in the building."

What can you tell us?

General TAYLOR. Sir, I will ask CSO McComb to comment further, but I believe it probably most appropriate to do this in the closed session as opposed to this open session to respond to that question.

Mr. HIGGINS. OK.

Colonel MCCOMB. Sir, what I would indicate is that, as you stated, you are correct in that there were two individuals that were discovered during our random screening processes as part of our enhanced security measures at the Nebraska Avenue complex, were discovered with weapons. The investigation is on-going, but as I indicated earlier, at this point there is no indication that either of these individuals were planning or conspiring to commit workplace violence. Both of these individuals recently had been previously cleared. As Under Secretary Taylor indicated, we certainly would be happy to provide more details of both of those events in the closed session.

Mr. HIGGINS. I have no further questions.

Mr. KING. Mr. Katko, the gentleman from New York.

Mr. KATKO. Thank you, Mr. Chairman.

General, it is good to see you again, Colonel McComb, and Rear Admiral Hayes.

Quick question for you. As you may know, I think you know, I have direct oversight over the Transportation Security Administration through my subcommittee. Is it fair to say that in your capacities, General and Colonel, that you consult TSA on a regular basis regarding intelligence matters and security matters?

General TAYLOR. Yes, sir, that is correct. Every day.

Mr. KATKO. OK, great. So just a couple of quick questions with respect to the insider threat at TSA facilities and airports.

I know you are well aware of the incident about a year-and-a-half ago where a fellow got off a plane in LaGuardia Airport with a backpack full of guns, and it turned out that an employee at the airport in Atlanta had carried those backpacks through the secure area using a SIDA badge and gave the backpack to the fellow and he brought it up to New York. It turns out that is about his tenth trip. The backpack in question had 16 guns, 9 millimeters and assault rifles, most of which were loaded. Obviously, that is a major concern about the insider threat from employees at airports.

Also, more recently, the insider threat at airports manifested with the Dallas-Fort Worth incident in a major drug trafficking case, which in the public record included invitations by one of the employees at the airport to bring anything through the access control areas, including bombs, if people wanted to.

With the threat from ISIS being what it is, and their desire to take down planes and taking credit for two planes that have been bombed in the last 8 months and perhaps even a third with EgyptAir, we don't know yet, it is a very real concern for me and it is something that I can't get over and I will continue to pursue.

The concerns are manifested for this hearing in two ways. One is the safety and security of the airports in the United States and the safety and security at last point of departure at airports worldwide.

With respect to the safety and security of the airports in the United States, are you aware of any changes in procedures that have been undertaken by TSA and/or Homeland Security with respect to the vetting of employees at airports; not just TSA employees, but vetting the employees at airports to ensuring that the insider threat is minimized?

No. 2, what do you think about beefing up the access controls for those employees?

General TAYLOR. Thank you for your question, Congressman. Some of this we would probably want to discuss in the closed hearing because of the sensitive nature of it.

But since the event in Atlanta, TSA has been working with the airport authorities and the Federal security directors to tighten up significantly the security in the sterile area, particularly for employees that have access under SIDA badges. We can speak to you about how those changes have occurred over time.

We are very much concerned about security in the open area, before the secure and sterile area, and we have communicated with airport operators and our Federal security directors continuously since Istanbul about that concern. We issued a joint NCTC, FBI, DHS joint intelligence bulletin around tactics, techniques, and procedures that we noted from Istanbul that we think will be valuable in planning security in the public areas of the airport.

It is a huge problem, we recognize that, and we will be consulting in the next month across the industry in terms of best practices for keeping the area open and welcoming, but also providing the layers of security that are necessary to protect the public that is there.

Mr. KATKO. Thank you.

Colonel, do you want to add anything or does that adequately cover it?

Colonel MCCOMB. The only thing I would add, sir, is that TSA does have a robust insider threat program. As we will talk in more detail in the closed session, they are very concerned about the areas that you discussed, and that will be a very prominent part of what they monitor as we continue to roll out and mature the Insider Threat Program within the Department of Homeland Security.

Mr. KATKO. If the Chairman will just indulge me one more moment.

Mr. KING. Sure.

Mr. KATKO. Thank you.

Just switching gears briefly, I am vitally concerned about developing facts with respect to opening the airports in Cuba. My concern is, quite frankly, that we are sprinting to the starting line, but we do not know where the finish line is, and I think it is a recipe for disaster. One of the biggest concerns I have is the insider threat at the airports in Cuba and the lack of appropriate facilities for those airports.

The Homeland Security Committee—Homeland Security I know is well aware of my concerns, but I just want to state them again on the record, Colonel and General. It is incredibly important that we do a thorough job evaluating those airports before we open up those routes. I know everyone is licking their chops from a financial standpoint and I know there may be some pressure from the administration because the President wants this done before he leaves office, but I urge you in the strongest words possible, based on everything I know, and we can talk more about that in a secure setting, that it is a very serious security issue.

One thing I can say on the public record is, when you don't even know how the Cuban officials screen their employees and they won't tell you how they do it and you don't know such basically things as that, I would strongly urge you that if you really are serious about the insider threat and you are very serious about keeping the skies safe, that you look at with a very focused eye on what is going on in Cuba before you open up those airports, with 20 direct flights a day to New York and possibly direct flights to Washington, which are the two main targets for terrorists.

General TAYLOR. Yes, sir. I think we can have a further discussion in the closed session about those challenges with those airports.

But for the record, DHS takes aviation security very seriously, particularly any aviation operating directly into the United States. We recognize the risk and want to make sure we have done a thorough job of assessing both the security at the airport and the security of the aircraft before they arrive here.

Mr. KATKO. Thank you very much. I yield back.

Mr. KING. The gentleman yields.

The gentlelady from Texas is recognized for 5 minutes.

Ms. JACKSON LEE. I thank the Chairman and the Ranking Member for this combined committee, and thank the witnesses, as well, for your presence here today.

Let me say that in the backdrop of the memorial yesterday that I attended in my home State for the fallen officers, let me again offer my deepest sympathy to the Dallas Police Department and to

the families who have lost loved ones through actions of terror and certainly through our recent incidences in our Nation that have befallen many families from many different States and jurisdictions.

That the climate that we are in calls for greater attention. Maybe as we speak we are not poignantly talking about the immediacy of loss of life, but cybersecurity incidences and intrusion to places where individuals should not go can certainly bring about an enormous amount of danger and possible injury and death.

I would like to put into the record—I am not sure if this is in the record—"Another Employee With A Gun Arrested At Homeland Security Headquarters, A Man Caught During Random Employee Screening." I would ask unanimous consent to put this into the record.

Mr. KING. We have already discussed that, but no objection.

[The information referred to follows:]

ARTICLE SUBMITTED BY HON. SHEILA JACKSON LEE

ANOTHER EMPLOYEE WITH A GUN ARRESTED AT HOMELAND SECURITY HEADQUARTERS

MAN CAUGHT DURING RANDOM EMPLOYEE SCREENING

By Scott MacFarlane

http://www.nbcwashington.com/investigations/Another-Employee-With-A-Gun-Arrested-At-Homeland-Security-Headquarters-386519051.html

For the second time in a month, an employee has been arrested for taking a handgun on to the secured grounds of U.S. Department of Homeland Security headquarters in Washington, D.C.

According to police and court records obtained by the News4 I-Team, security officers arrested Thomas Pressley of Woodbridge, Virginia, Monday, accusing him of carrying a 9-millimeter handgun in a leather handbag while inside the complex.

Feds Request Stay Away Order for DHS Employee Arrested

Pressley, a contractor who works in IT for the agency, has been ordered jailed in D.C. until his next scheduled court appearance Friday. He is charged with carrying a pistol without a license. Court filings did not detail what, if any, plea has been entered in the case by Pressley. His attorney did not immediately return requests for comment from the I-Team.

Federal government records specify the U.S. Department of Homeland Security headquarters complex on Nebraska Avenue in northwest Washington is among the most secured government facilities in the United States, rivaling the security apparatus of the White House and the Pentagon.

Feds Investigating Whether Employee Was Plotting Attack on DHS Officials

"The weapon appeared to be fully functional, capable of being fired by a single hand, and designed to expel a projectile by the action of an explosive," according to a police report.

The report also said, "The weapon also had a barrel length of less than 12 inches."

DHS Employee Found With Gun at HQ

Agency security located the handgun during a random employee screening, the report said.

"As a result of enhanced security and screening measures at the NAC, security officers detained a contract employee yesterday after they discovered a concealed firearm during screening," a DHS spokesman said. "The contract employee was subsequently arrested.

"While we currently have no information to suggest that this individual sought to cause harm, as discussed at a recent employee town hall, the safety of employees and visitors to DHS facilities is a top priority. The enhanced security procedures discussed at that meeting remain in effect, including increased levels of screening of employees entering the NAC. And because we won't hesitate to take every appropriate measure to protect our employees, our security professionals are evaluating what additional security enhancements may be necessary."

Pressley's arrest comes about a month after the arrest of Jonathan Wienke, another Homeland Security employee accused of carrying a firearm inside agency headquarters. Court filings from investigators said Wienke was found with a loaded .22-caliber handgun, carrying five hollow point bullets in June.

Wienke pleaded not guilty to a gun charge and is awaiting further court proceedings in the case.

But Wienke had more than a gun when he was searched on June 9, according to a request for court permission to raid Wienke's home. A federal agent and security officers also found Wienke had a knife, pepper spray, thermal imaging equipment and radio devices.

And the feds said in the court filing that Wienke was found in his workspace, which is in close proximity to a meeting of senior agency officials the day of his arrest—and that Wienke was aware of the meeting.

In the same court filing, the agent said there was "probable cause to believe Jonathan Wienke was conspiring with another to commit workplace violence and, more particularly, may have been conspiring or planning to commit violence against the senior DHS officials in the building."

Ms. JACKSON LEE. All right. Put the story at least into the record. The reason I say that is because there are a number of intrusions that I am concerned about and I want to discuss some legislation that I have introduced as well.

But let me pointedly go to two entities, nations that are known as our chief threats to intelligence assets of the United States, and this would be to you, Mr. Secretary, Secretary Taylor. How can Russia or China use the OPM breach data with the Ashley Madison breach of information to compromise security?

General TAYLOR. Ma'am, I would prefer we respond to that question in the closed session. I think we can be more full in our answer.

The threat from cybersecurity is a significant threat and the information and data that is collected through cyber intrusion means present a significant threat to our country. But the specifics, I would prefer if we could answer that in the closed session.

Ms. JACKSON LEE. OK. Well, let me just get a general assessment then, because I am not sure when we will designate a closed session.

Mr. KING. Right after this, as soon as you are finished, we are going downstairs.

Ms. JACKSON LEE. OK. Then let me just make my own comments and say the great concern that I have of that data being out is what I hope that we will have a focused perspective on—and I assume that you can answer—we will have a focused effort on that.

General TAYLOR. We have 110 percent focused effort on that activity and the potential implications of that activity for the National security.

Ms. JACKSON LEE. Very good.

Let me then go to some legislation that I think had to do or reflects the shooter that was at the Navy Yard and Snowden. As I understand, they were vetted for security by the same contractor.

Are you able to comment on any firewalls that are being put on outside contractors, any extensive review on contractors who have responsibilities for vetting and where the Government relies upon them? Are these contracts periodic? Do people get 10-year contracts? Are these people wedded in their positions, can't be taken out? Are they lax? What is happening?

I think that Snowden has to be one of the most severe and outrageous responses or actions that we had in security and he was

vetted and he was engaged in, I think, at too high a level of the Nation's security data, intelligence data.

Colonel MCCOMB. Ma'am, kind of bottom-line up-front is that the vetting of contractors and the companies that have contractors are done in accordance with the Federal Investigative Standards. At the interagency level, the Performance Accountability Council for suitability, security clearances, and credentialing is looking at that issue very hard.

All of the companies who are on Classified contracts must meet the National Industrial Security Program standards, which requires that they have a facility security officer, they run through the background investigations of the individuals who will be working those contracts, whether they be for an investigative purposes or if they are doing some other level of work, whether it be on the IT systems, et cetera.

We in DHS look at those contractors from a fitness perspective, once again applying the OPM standards. So we look at that very hard. Contracts are held to the standards that are in the performance work statement. Where there are issues or breaches of those, then contracting action can be taken against those individuals, those companies, to include termination on behalf of the Government based on those breaches.

We continue to monitor that along with the contracting folks. The other thing I would add is, with the cyber hygiene initiative in the Department of Homeland Security we are ensuring that all information that is handled through contracts is kept at the high security level, which is above the standard required for the Federal Government, to ensure that it is protected at the appropriate levels and that it is not potentially endangered for unauthorized access.

Ms. JACKSON LEE. Can I get just a quick follow-up, Mr. Chairman, just very quickly?

Mr. Snowden was lodged somewhere in the back corners of a Hawaii office building. Do you have the responsibility—and you are one of the intelligence components, I understand that—but the monitoring? You may have the company and then you have these individual actors under the company, maybe many. Is there a mode of monitoring those individuals?

Last, if our cyber system is attacked, meaning what we utilize here in the Government, are we prepared? That may be an answer for a back-up system somewhere.

General TAYLOR. Ma'am, I will try to answer your question.

First, our insider threat monitoring will monitor everyone that has access to our Classified systems—contractor, Government employee, regardless—and ultimately individuals that are operating on our Unclassified system that may or may not have a security clearance.

Cyber hygiene has been a real focus of Secretary Johnson with regard to applying the National programs division cybersecurity initiatives across our Government and ensuring that they are robustly applied and effectively implemented.

So it has been a major focus for us. I can't speak to the issue of back-up. I am not technically qualified to understand that system. But would certainly find the answer to that question for you and get back to you, ma'am.

Ms. JACKSON LEE. I would appreciate it. Thank you.

Did you want to answer?

Colonel MCCOMB. No, ma'am.

Ms. JACKSON LEE. All right.

Thank you all for your testimony.

Mr. Chairman, may I ask, I won't pursue the back-up system. Maybe I will get that at another time.

Mr. KING. OK. We have to start going downstairs soon.

Ms. JACKSON LEE. Yes. Let me ask unanimous consent to put in the record, *Bloomberg News,* "Edward Snowden and the NSA: A Lesson About Insider Threats." I ask unanimous consent.

Mr. KING. Without objection.

[The information referred to follows:]

ARTICLE SUBMITTED BY HON. SHEILA JACKSON LEE

EDWARD SNOWDEN AND THE NSA: A LESSON ABOUT INSIDER THREATS

Vijay Basani, Bloomberg News, July 3, 2013

https://www.bloomberg.com/news/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-about-insider-threats

In all the mysteries surrounding the Edward Snowden affair, there's one that hasn't received much attention: Why didn't the NSA, one of the most technologically sophisticated organizations on the planet, have a way to detect that Snowden was downloading thousands of documents?

The corollary question every chief executive should ask of his or her top security officer: "Does our organization have a way to detect unauthorized access to our data?" According to the recent SANS 2013 Critical Security Controls survey, less than 10 percent of companies actually have proactive monitoring of security controls, the area that governs unauthorized access.

Employees and contractors with boundless privilege to access sensitive data present greater risk of intentionally, accidentally, or indirectly misusing that privilege and potentially stealing, deleting, or modifying data. Human nature is the weakest link when it comes to the intersection of people, process, and technology—the three tenants of security—and the Edward Snowden blunder is a perfect example.

According to Michael Hayden, former director of the NSA and the CIA, no more than 22 personnel at NSA were to have access to the highly Classified data, which included about 1 billion-plus records per day. One can assume that these individuals should be internal analysts who have gone through extensive background checks, who are very experienced in dealing with highly confidential data, and who are employees of NSA. We can also assume that these individuals have special privileges to access these data in a highly secure manner.

I have no special knowledge of the NSA's internal workings, but it appears that somehow this protocol was not followed, and Snowden, a contractor, was given access to this information with no mandatory monitoring, a clear violation of controls and a breakdown of process.

While technologies do exist to enforce access rights, privileges, and policies, the technology is only as good as the people and processes that are put into place. If people who manage these technologies decide to circumvent the technology's ability to enforce policies, or make an exception, or ignore violations, or do not instill sufficient supervisory mechanisms, then the technology will fail.

Another issue to be looked at from a technological perspective is the complete lack of continuous monitoring and auditing of the users, process, and security controls in a unified fashion by the NSA.

If someone at the NSA were monitoring, analyzing, and auditing all network, user, and system activity, policy enforcements, etc., to identify abnormal behavior and usage patterns, most likely Snowden's access to sensitive data, the connection of removable media and copying of these data would have drawn red flags. It is possible that the data and signals from individual products, such as a USB monitoring solution or a database activity monitoring system, would have captured these data, but the individual administrators who were looking at each data point in isolation were not able to connect the dots. If the NSA had adopted technology that pulled

all information into a single database and automatically correlated the data in a unified fashion, it would have detected a potential breach or policy violation.

Unfortunately the Snowden situation of privileged access to sensitive data with lack of sufficient checks and balances is an all-too-familiar story in the private sector. Executive management tends to have a checkbox mentality when it comes to security (i.e. do what is absolutely necessary to pass a government or industry mandate) or lack the knowledge to realize that their intellectual property and business is at risk for lack of sufficient security controls.

With traditional network perimeters becoming increasingly porous with the introduction of BYOD, mobile devices, and cloud infrastructure, organizations need to implement security best practices, such as SANS 20 Critical Security Controls, to protect against cyber attacks and espionage. This requires resources and budget commitment from C-level management.

The Snowden debacle should be a wake-up call in both the public and private sectors to adopt an approach that provides complete awareness and continuous, automated monitoring of critical security controls to reduce real risk and real threats to their business.

Ms. JACKSON LEE. I yield back.

Mr. KING. I ask unanimous consent that the remainder of the hearing be closed to the public under House Rule XI, clause 2(g)(2), because disclosure of testimony, evidence, or other matters would endanger National security or compromise sensitive law enforcement information.

Is there any objection to the motion to close the hearing?

Hearing none, the motion is agreed to, and the subcommittee will recess briefly to move to a more secure location to continue its business. The hearing will reconvene in that location in 15 minutes.

[Whereupon, at 10:50 a.m., the subcommittee proceeded to closed session and subsequently adjourned at 11:27 p.m.]

○