WRITTEN TESTIMONY OF

Gregory Marshall

Chief Security Officer

Management Directorate

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Homeland Security (CHS)

November 13, 2013

311 Cannon House Office Building

Chairman King, Ranking Member Higgins, members of the Committee, good morning and thank you for the opportunity to provide testimony on personnel security.

I am Greg Marshall, Chief Security Officer of the U.S. Department of Homeland Security (DHS). I lead the dedicated men and women who make up the Office of the Chief Security Officer. My office is an element of the Department's Management Directorate, and I report to the Under Secretary for Management.

The mission of our office is to safeguard the Department's people, property, information, and systems. Accordingly, the DHS Chief Security Officer is responsible for security-related issues affecting the more than 235,000 DHS employees that compose the Department. I exercise DHS-wide security program authorities in the areas of personnel security, physical security, administrative security, special security, identity management, special access programs, and security training and awareness. I also support the Chief Information Officer in the area of IT security policy and the Under Secretary for Intelligence and Analysis in the protection of intelligence sources and methods, and accreditations of classified facilities.

The security oversight and guidance authority of my office applies across the Department. However, Operational Components play a significant role in managing the facilities which they inhabit, including access to those facilities. The diverse missions and responsibilities of the Department underscore the challenges involved within the physical security and access control disciplines.

The tragic events of Monday, September 16th at the Washington Navy Yard have placed the issue of physical security, access control, and personnel vetting front and center in the minds of security professionals across the federal landscape.

Shortly after the Navy yard incident, I convened a meeting of the Department's Chief Security Officer Council. Each Component Chief Security Officer (CSO) acknowledged the significance of the Navy Yard tragedy to access control and the underlying vetting processes and each CSO commented on the complexities of vetting and access, including the costs involved. With this in mind, the Department remains committed to ensuring that only those persons with a legitimate need to access any given facility are allowed to enter, that those persons possess no prohibited items, and that the backgrounds of those persons who do enter have been vetted to an appropriate level of rigor.

I would make clear, however, that security involves risk management. Our job is to do everything we can to reduce the risk and keep our employees safe. In pursuit of our mission, please be assured that DHS security leadership and the professionals we manage have the benefit of extensive knowledge, training, and experience. We also have the benefit of comprehensive policies, procedures, processes, and emerging technologies to help guide and improve our key security programs.

For example, when we consider the security posture for a federal facility, including access control, we at DHS follow Interagency Security Committee standards. During this process, facilities are assessed for risk, and appropriate countermeasures are employed to mitigate the risks. Using a decision matrix involving mission criticality, the sensitivity of the activities conducted, threats to the facility, facility population of persons who work and visit there, and other factors, an appropriate Federal Security Level is assigned to each facility. Accordingly, the outcomes of these risk assessments drive the level of protection for each facility, to include an appropriate access control posture. Simply put, a one-size security solution does not and cannot fit all facilities.

For our employees to qualify for access to a federal DHS facility, an employee must undergo a background investigation to establish his or her suitability for employment. These investigations are, for the most part, conducted by OPM on behalf of DHS. Contractors are screened in a process similar to employees in order to determine their fitness to work on a DHS contract and have unescorted access to DHS facilities. Background investigations for suitability and fitness examine character and conduct behaviors, such as criminal history, alcohol and drug use, and employment history, among others. Based upon all available information, a personnel security specialist makes an adjudicative decision concerning a person's suitability or fitness for employment, including access to facilities.

It is important to understand that a background investigation for suitability and one for a security clearance processes with multiple levels of investigation dependent upon the access required and level of risk. A security clearance allows access to classified information, while a favorable suitability or fitness determination allows employment and access to facilities. On its own, a background investigation for suitability does not permit access to classified information.

It is also important to note that a background investigation for either a suitability determination or a security clearance, no matter how rigorous, is no guarantee that every bit of relevant information about the individual is available or has been included. For example, prior criminal convictions and/or arrest information may not be reported in state and/or federal repositories, often simply due to data entry resource constraints. It is these types of checks that are basic elements of any federal employment background investigation.

Also, it is important to note that a background investigation may not be an indicator of future behavior. Even those who have successfully undergone the most rigorous set of background

checks available – even a comprehensive polygraph examination – may someday prove untrustworthy. Ultimately, a federal background investigation only examines past behavior and is sometimes based on limited available information.

A federal background investigation is an exercise in risk management, establishing some basic facts such as identity, citizenship, criminal history, etc. However, a background investigation cannot be characterized, in and of itself, does not guarantee any single individual's continuing day-to-day fitness to carry out his or her employment responsibilities or to behave in a lawful and safe manner.

With these limitations in mind, there have been several recent improvements to the ability of the government to manage these inherent risks.

First, Homeland Security Presidential Directive 12 (HSPD-12) mandated the development and implementation of a government-wide standard for a secure and reliable Personal Identity Verification (PIV) card for gaining access to federally-controlled facilities. To date, DHS Headquarters and Components have issued over 250,000 PIV cards to federal employees and contractors. For the first time, this process has effectively linked the completion of a person's background investigation with the issuance to that person of a unique federal identity credential. The PIV card represents a marked improvement over the various legacy access/identity cards, but is only a part of any solution. As a result, federal facility access control processes use this PIV card and its various authentication mechanisms to verify the identity of the holder, link the holder to the card, and link the card itself to a database of valid employees and contractors having legitimate business at any given facility.

Second, the background investigation process itself is undergoing a major government-wide reform effort, to include revised federal investigative standards signed jointly by the Director of National Intelligence and the Director of the Office of Personnel Management in 2012, and phased implementation to begin this fiscal year. With the federal investigative standards, the concept of "continuous evaluation" is being developed to supplement the normal re-investigation reviews of employees which, under the revised standards, will be in five-year increments, with a government-led process that examines a person's conduct within his or her normal re-investigation timeframes. As such, relevant security information like a recent arrest or conviction for a crime outside of the federal system, for example, would become available on a timelier basis to security officials responsible for assessing a person's eligibility for access to classified information, thereby helping to ensure that classified information and/or federal facilities are appropriately safeguarded. "Continuous evaluation" represents a significant process improvement over current capabilities and will mitigate some of the limitations in the existing background investigation process discussed above.

Finally, this Administration's recent Information Sharing and Safeguarding initiative, also known as "Insider Threat," seeks to complement background investigations and continuous evaluation with continuous monitoring. Continuous monitoring will incorporate data in near real-time from a much broader set of data sources, as compared to information that was previously available in the background investigation process. The initiative focuses on monitoring certain IT systems and incorporates analysis and collation software to aid in the identification of behavioral trends that could be indicative of an insider threat problem. Strict referral protocols are in place to investigate abnormalities.. The aim is the detection and mitigation of threats to classified information before any damage can be done. The focus of this program is the protection of

classified information, but its applicability to other behavioral issues, including suitability and contractor fitness, is evident.

In conclusion, the suitability determinations of and access control to federal facilities by federal employees and contractors remains a work in progress, but is evolving toward dramatic improvement. It is our responsibility as DHS security leaders, with the support of Congress, to ensure a safe and secure workplace. We have made important strides, but assessing and managing employee and facility risks will continue to be a challenge in the future. We will continue to work every day to meet these challenges. Thank you again for the opportunity to testify today.