Statement of

Mr. Stephen F. Lewis
Deputy Director for Personnel, Industrial and Physical Security Policy
Directorate of Security Policy & Oversight
Office of the Under Secretary of Defense for Intelligence

before the
Homeland Security and Governmental Affairs Committee
United States Senate
on

Tuesday, December 17, 2013

Good Morning,

Thank you, Chairman Carper, Ranking Member Coburn and distinguished Members of the Committee –I appreciate the opportunity to appear before you today to address the practices and procedures in the Department of Defense (DoD) regarding facility security. I am Steve Lewis, Deputy Director of the Security Policy and Oversight Directorate in the Office of the Under Secretary of Defense for Intelligence, and I am here today on behalf of Under Secretary of Defense for Intelligence (USD(I)), Michael Vickers.

The USD(I) is the Principal Staff Assistant to the Secretary and Deputy Secretary of Defense for security matters and is responsible for setting overall DoD physical security policy. In this role, the USD(I) provides security policy standards for the protection of DoD personnel, installations, facilities, operations and related assets.

Within the Department, the USD(I)'s security responsibilities are complemented by those of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD & ASA)), who is responsible for the DoD Antiterrorism (AT) Program. The DoD AT Program is an element of the Department's defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.

In the wake of the recent Washington Navy Yard shooting incident, the Secretary of Defense initiated concurrent independent and internal reviews to identify and recommend actions that addresses gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel. The Deputy Secretary of Defense will consolidate key recommendations from each of these reviews into a final report to be provided to the Secretary of Defense. If approved, these recommendations will be addressed in an implementation plan, in coordination with the DoD Components and key Federal agency partners as appropriate.

In order to address the Department's facility security policies and practices, I believe it is important to first describe the requirement for military commanders (or civilian equivalents) to conduct a comprehensive evaluation of an installation, facility, or activity to determine its ability to deter, withstand, and /or recover from

the full range of adversarial capabilities based upon a threat assessment, compliance with established protection standards, and risk management. Based upon the results of these evaluations, active and passive measures are designed to safeguard and prevent unauthorized access to personnel, equipment, installations, and information by employing a layered security concept (i.e., security-in-depth).

With regard to security plans, the Department requires the development and maintenance of comprehensive plans to address a broad spectrum of natural and man-made scenarios. These include the development of joint response plans to adverse or terrorist incidents, such as active-shooter incidents, chemical/biological attacks, unauthorized access to facilities, and tests of physical security. Military commanders (or civilian equivalents), using risk-management principles, are required to conduct an annual local vulnerability assessment, and are subject every three years to a Higher-Headquarters Assessment, such as the Joint Staff Integrated Vulnerability Assessment (JSIVA). A JSIVA is a “vulnerability-based” evaluation of an installation's ability to deter and/or respond to a terrorist incident. Vulnerability-based assessments consider both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, in terms of their mobility and the types of weapons historically employed.

The Department has worked very hard to foster improvements that produce greater efficiencies and effectiveness in facility security. In its continuing efforts to

harmonize its facility security posture with other Federal departments/agencies, military commanders (or civilian equivalents) located in DoD-occupied leased facility space, including U.S. General Services Administration-owned facilities not on a DoD installation, must utilize the Federal Interagency Security Committee's (ISC) Risk Management process for Federal Buildings. This effort includes the incorporation of the ISC's physical security standards in relevant Department guidance documents (i.e., Unified Facilities Criteria).

We participate in various interagency forums such as the Interagency Security Committee, and Government Facilities and Defense Industrial Base Critical Infrastructure Sector Partnerships, along with representatives from the Department of Homeland Security and other senior-level executives from 53 Federal Agencies/departments. These forums enable the sharing of best practices, physical security standards, and cyber and terrorist threat information in support of our collective resolve to enhance the quality and effectiveness of physical security of Federal facilities.

We have various ongoing initiatives across the Department to enhance facility security, such as the development of an Identity Management Enterprise Services Architecture (IMESA) that will provide an enterprise approach to the sharing of identity and physical access control information, as well as complement ongoing continuous evaluation concept demonstration efforts. The IMESA capability will provide real-time vetting of individuals requiring unescorted access

to DoD facilities against DoD, other Federal, State, and local authoritative data sources. Secure information sharing will enable those facilities with physical access control systems to authenticate individuals' access credentials, authorization, and fitness to enter the facility, vastly enhancing the security of DoD personnel and resources worldwide.

Thank you for your time. I am happy to take your questions.