FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE COMMITTEE ON HOMELAND SECURITY
AND
SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Statement by

The Honorable Paul Stockton

Assistant Secretary of Defense for Homeland Defense

and Americas' Security Affairs

Before the 112th Congress

Committee on Homeland Security

U.S. House of Representatives

and the

Committee on Homeland Security and Governmental Affairs

United States Senate

December 7, 2011

Chairman King, Chairman Lieberman, Ranking Member Thompson, Ranking Member Collins, distinguished members of the Committees: thank you for the opportunity to address you today on the homegrown terrorist threat to military communities inside the United States. Let me provide you with my bottom line up front. The terrorist threat to our military communities is serious, and will remain so for years to come. The Department of Defense (DoD) has greatly improved its ability to meet this threat, through internal initiatives and partnerships with the Department of Justice, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) including U.S. Immigration and Customs Enforcement (ICE), and law enforcement agencies across the Nation. This is no time to rest on our accomplishments, however. With your help, and with the strong support of the leadership of my Department, I pledge to continue to strengthen the preparedness of our domestic military communities against the enduring, evolving threats of terrorism they confront.

When it comes to defining the enemy, this Administration wishes to avoid imprecise terminology that may cause confusion and may unjustifiably give credence to the falsehood – despite our best intentions – that we are waging a war on Islam. Muslim-Americans are important allies in the effort to counter violent extremism in the United States. This is consistent with the Administration's strategy "*Empowering Local Partners to Prevent Violent Extremism in the United States*" which affirms, "The best defenses against violent extremist ideologies are well-informed and equipped families, local communities, and local institutions." Muslim-Americans are also important in DoD operations. Every day, patriotic Muslim-Americans serve in our military, often providing linguistic and cultural competencies essential to disrupting and defeating our actual enemy: al Qaeda and its adherents and affiliates worldwide.

Deputy National Security Advisor Denis McDonough noted in March 2011 that "Al Qaeda and its adherents are constantly trying to exploit any vulnerability in our open society. This threat is real, and it is serious. How do we know this? Well, al Qaeda tells us. They make videos, create internet forums, even publish online magazines, all for the expressed purpose of trying to convince Muslim Americans to reject their country and attack their fellow Americans." The Department of Defense faces a special challenge in this regard. Al Qaeda and its affiliates seek to inspire and instruct U.S. military personnel and other radicalized U.S. citizens to conduct "lone actor" attacks on U.S. military targets. These adherents are, as Deputy National Security

Advisor John Brennan has said, "individuals, sometimes with little or no direct physical contact with al Qaeda, who have succumbed to [al Qaeda's] hateful ideology and who have engaged in, or facilitated, terrorist activities here in the United States … and we have seen the tragic results, with the murder of a military recruiter in Arkansas two years ago and the attack on our servicemen and women at Fort Hood."[1]

As noted in a White House statement in August 2011: "The past several years have seen increased numbers of American citizens or residents inspired by al-Qaeda's ideology and involved in terrorism."[2] Over the last decade, a plurality of these domestic violent extremists chose to target the Department of Defense (DoD), making military communities the target of choice for homegrown terrorists. Fourteen of seventeen Americans killed in the homeland by domestic violent extremists have been DoD personnel.

As President Obama said in September, "The death of [Anwar al-Awlaki] was a major blow to al Qaeda's most active operational affiliate. Awlaki was the leader of external operations for al Qaeda in the Arabian Peninsula. In that role, he took the lead in planning and directing efforts to murder innocent Americans." The fact that al-Qaeda's adherents are openly and specifically recruiting Americans to support or commit acts of violence—through videos, magazines, and online forums—poses an ongoing and real threat.[3]

As acknowledged in the June 2011 National Strategy for Counterterrorism, "[m]ass media and the Internet in particular have emerged as enablers for terrorist planning, facilitation, and communication … Global communications and connectivity place [al Qaeda's] calls for violence and instructions for carrying it out within easy reach of millions." Given the adversary's emphasis on recruiting U.S. military personnel to attack our communities from within, the Department has taken numerous actions to broaden its approach to force protection beyond its traditional focus on external threats.

---

[1] Brennan, John. Remarks on Ensuring al-Qa'ida's Demise" as prepared for delivery, Paul H. Nitze School of Advanced International Studies. Washington, D.C. June 29, 2011.
[2] The White House. Empowering Local Partners to Prevent Violent Extremism in the United States. Washington: August 2011.
[3] The White House. Empowering Local Partners to Prevent Violent Extremism in the United States. Washington: August 2011.

After the tragic shooting at Fort Hood, then-Secretary Gates commissioned the DoD Independent Review Related to Fort Hood to identify gaps and deficiencies in DoD's force protection programs, policies, and procedures. In response to the Independent Review's recommendations, then-Secretary Gates directed that the Department make every effort to safeguard civil rights and civil liberties while implementing several specific actions to adapt effectively to the challenging security environment in which we operate. These initiatives will significantly improve the Department's ability to mitigate internal threats, ensure force protection, enable emergency response, and provide care for victims and families should another attack occur.

It is important to recognize that although al Qaeda and its affiliates and adherents currently pose the preeminent security threat to the United States, history has shown that the prevalence of particular violent extremist ideologies changes over time, and new threats will undoubtedly arise in the future.[4] The July 2011 tragedy in Norway and the April 1995 Oklahoma City bombing underscore this point. The Administration's August 2011 strategy, *Empowering Local Partners to Prevent Violent Extremism in the United States*, provides a useful definition for violent extremists: "individuals who support or commit ideologically-motivated violence to further political goals." Though the nature and significance of these threats can vary, our obligation to protect the American people demands that we maintain a strategy that counters all of them. Consistent with the "Empowering Local Partners to Prevent Violent Extremism in the United States" the Department of Defense's initiatives address the range of violent extremist threats we face.

As a matter of law and national policy, DoD is generally restricted from collecting and storing law enforcement information on U.S. citizens; therefore, DoD must rely on civilian agencies to play an increasingly important role in the protection of U.S. military communities. As part of the Fort Hood review, then-Secretary Gates directed several actions to improve DoD collaboration with the Federal Bureau of Investigation (FBI). Effective August 2011, the Attorney General and the Secretary of Defense implemented a single, overarching information-sharing Memorandum of Understanding (MOU) to promote systemic, standardized, and

[4] The White House. Empowering Local Partners to Prevent Violent Extremism in the United States. Washington: August 2011.

controlled information sharing. This MOU establishes a general adjudication process whereby DOD and the FBI can resolve potential future differences of opinion to whether and when information should be shared.

This MOU will be supplemented by a series of specific annexes, several of which are in the final stages of negotiation before proceeding to signature. These annexes will clarify coordination procedures and investigative responsibilities between DoD and the FBI. Most significantly, Annex A, "Counterterrorism Information Sharing," will allow DoD to articulate its force protection information requirements to eliminate confusion or doubt about what threat information is considered to be of value to DoD. Threat information with a DoD nexus is shared at the institutional level and at the local level. As a result, DOD will be able to evaluate the threat information from a high-level perspective to "connect the dots" more effectively. At the same time, installation commanders have the information they need to take appropriate force protection and antiterrorism measures to protect their communities from the threat. We anticipate this Annex will be signed early next year.

We also have drafted an annex addressing Counterintelligence Information Sharing (Annex B) that we anticipate will be signed by January 2012. Additional annexes addressing the subjects of "Terrorist Screening Information" and "DoD Participation in FBI Joint Terrorism Task Forces" will enter coordination shortly. Once the "DoD Participation in FBI Joint Terrorism Task Forces" annex is finalized, we will publish a conforming DoD Instruction, "DoD Support to the Federal Bureau of Investigation Joint Terrorism Task Force Program," which will provide policy and guidance for each DoD component represented in the FBI's Joint Terrorism Task Forces (JTTFs). By Fiscal Year 2015, DoD will provide approximately 123 detailees to support 60 FBI JTTFs throughout the United States. The FBI has instituted a formal training program to ensure these DoD professionals are familiar with all available JTTF tools, databases, and information.

DoD is also working closely with State and local law enforcement agencies to recognize the indicators of a "lone actor" threat and to share suspicious activity reports to prevent another Fort Hood-type of attack from occurring. In September 2010, DoD began using eGuardian, an unclassified, secure, web-based capability to report suspicious activity that can be accessed

through the Law Enforcement Online (LEO) network. eGuardian is part of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The eGuardian system appropriately safeguards privacy and civil liberties, enabling information sharing among Federal, State, local, and tribal law enforcement partners, including State and Major Urban Area Fusion Centers and the FBI JTTFs. When fully implemented in February 2012, eGuardian will have approximately 1500 DoD users worldwide, and all DoD law enforcement entities will have access. The system was designed to remedy information-sharing gaps that the review of the Fort Hood shootings revealed and has already resulted in at least 384 new investigations or case enhancements. In addition, DoD is working to identify funding for the Defense Data Exchange (D-DEx), which will allow all 13 DoD law enforcement entities to post and query criminal investigation and other law enforcement data in a single repository.

DoD is also acting on lessons learned. For instance, the Independent Review related to Fort Hood ("Protecting the Force: Lessons from Fort Hood") found DoD force protection policies and programs were not sufficiently focused on internal threats. To improve intradepartmental information sharing on insider threats, as well as to synchronize force protection and law enforcement policies and programs across DoD, we established a permanent Force Protection Senior Steering Group (FP SSG). My office and the Joint Staff co-chair the FP SSG, which meets not less than semiannually and reports progress and recommendations to the Deputy Secretary's Defense Management Action Group (formerly known as the Defense Advisory Working Group).

The FP SSG has an "Insider Threat Working Group" (or "InTWG"), which includes representatives from the Joint Staff, the Military Departments and Services, and most DoD components. The InTWG examines the insider threat from three perspectives: (1) workplace violence, (2) terrorism, and (3) security threats (including espionage and threats to information systems). unique among other similar Federal Government insider threat working groups, the InTWG addresses both kinetic and non-kinetic insider threats. The InTWG is drafting a DoD Instruction to provide guidance that will improve information sharing among DoD law enforcement and intelligence entities and establish a single, DoD-wide definition of insider threat as: "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data

modification, espionage, terrorism, or kinetic actions resulting in personal injury or loss or degradation of resources or capabilities." Under this broad strategic umbrella, individual DoD components may initiate programs tailored to address their distinctive vulnerabilities.

In order to recognize potential threats before they materialize, DoD must first identify and validate behavioral indicators of, or precursors to, violent behavior. In August 2010, then-Secretary Gates issued interim guidance on how to identify and report potential insider threats. This guidance, developed in consultation with academic experts and law enforcement practitioners, familiarizes leaders with a list of behaviors that may indicate a potential propensity to commit violent acts. Behaviors on the list vary in degrees of severity—some behaviors are themselves illegal or violate DoD rules—others may be cause for concern only in certain contexts. Military personnel who exhibit indicators, such as hatred or intolerance of American society and culture, advocacy for violence-promoting organizations, and history of poor work performance or substance abuse problems, should elicit concern from commanders or supervisors. In all cases, leaders are expected to exercise proper judgment and consider the full range of administrative and disciplinary actions when addressing personnel whose behavior adversely affects good order, discipline, or safety of the unit. This interim guidance is intended to protect the force in the near term.

In April 2010, then-Secretary Gates approved the Defense Science Board (DSB) study on violent radicalization. In addition to validating indicators of violence, the DSB was asked to recommend training tools to enable commanders and supervisors to recognize when and how to intervene and thwart potential insider threats. I expect the DSB report to be completed in March 2012. In addition, the Assistant Secretary of Defense for Health Affairs will conduct two scientific studies – one retrospective and one prospective – to examine DoD populations and to develop a scientifically-based list of behavioral indicators of violence in the military population. As findings from these studies become available, DoD will refine its interim guidance to incorporate what we learn into other existing workplace violence prevention and intervention programs and policies. DoD has already supplemented pre- and post-deployment healthcare screening questionnaires to help healthcare providers assess the risk of violence by DoD personnel and to refer such personnel for further evaluation or treatment as necessary.

Although DoD's intent is to prevent insider threats from materializing, we have also taken several measures to improve emergency response when they do. Since March 2010, "Active Shooter" training has been an important component of mandatory Antiterrorism Level 1 training. Active Shooter best practices are being included in revisions to the minimum standards for military police (and equivalents).

Finally, DoD is implementing installation emergency management (IEM) programs, including "Enhanced 911," mass notification and warning systems, and a "common operating picture." "Enhanced 911" provides dispatchers with the caller's location, even during cell phone calls, which is especially important in case the caller becomes incapacitated. Mass notification and warning systems automate guidance (e.g., evacuation orders) to warn and direct installation personnel, helping emergency responders manage affected populations over the course of an incident. The "common operating picture" is intended to enable coordination among emergency responders by sharing information in real-time during an incident. This "common operating picture" is also intended to improve installations' capacity to report force protection information to the Combatant Commands. IEM program implementation will save lives, promote interoperability with civilian first responders, and ensure compliance with national preparedness and response guidelines.

Chairman King, Chairman Lieberman, Ranking Member Thompson, Ranking Member Collins, distinguished Members of the Committees: I commend you for your leadership, continued interest, and support of DoD's efforts on this important matter. We have an obligation to ensure that the men and women who are prepared to sacrifice so much for our Nation anywhere in the world are safe here at home.