

Statement by

Peter Verga

Principal Deputy Assistant Secretary of Defense for Homeland Defense

Before the 109th Congress

Committee on Armed Services

Subcommittee on Terrorism, Unconventional Threats and Capabilities

Committee on Homeland Security

Subcommittee on Emergency Preparedness, Science and Technology

United States House of Representatives

July 21, 2005

Introduction

Chairman Saxton, Representative Meehan, Chairman Cox, Representative Thompson, distinguished members: thank you for inviting me here to address you today.

For most of the 20th century, we knew who our enemies were and where they lived. The New York City and Pentagon terrorist attacks of September 11, 2001, the Madrid train bombing of March 2003, and, most recently, the tragic bombings in London heralded the emergence of a new enemy. In the smaller, more ambiguous, and more dangerous world of the 21st century, we are at war with an enemy with no countries, capitals, or populations to put at risk and no armies, navies, or air forces to attack. This enemy is a complex network of ideologically driven extremists who will attempt to engage us not only far from U.S. shores, but also here at home, employing asymmetric means to penetrate our defense and exploit the very openness of our society to their advantage.

To safeguard the American way of life and to secure our freedom we cannot depend on passive or reactive defenses. A new strategic imperative is necessary to successfully face this enemy and protect the United States and its citizens: we must actively confront – when possible, early and at a safe distance from our borders – our enemy and those who aid and abet them with all the instruments of our national power.

Protecting the United States

The Global War on Terror is the execution of this new 21st century strategic imperative. There is no “home game” or “away game” – we are engaged in a global conflict and must understand that the battlefield on which we must confront our enemy is also global in nature, involving multiple fronts, not just geographic theaters. Nor are the multiple fronts of this global conflict primarily military. The

Global War on Terror involves complementary elements of America's power, with the military playing a critical, but by no means exclusive, role, along with intelligence, law enforcement, and diplomacy. The main elements of our national strategy in this global conflict include: (1) protecting the homeland; (2) disrupting and attacking terrorist networks; and (3) countering ideological support for terrorism.

The Department's paramount goal, in accordance with the 2005 National Defense Strategy, is the protection of the United States from direct attack. We give top priority to dissuading, deterring, and defeating those who would seek to harm the United States directly, especially enemies with weapons of mass destruction (WMD). Homeland defense must be understood as an integral part of a global, active, layered defense – a defense in depth – of the United States, that is focused on securing the United States and its citizens from attack. Defense of our nation actually starts abroad, where our soldiers, sailors, airmen, and Marines put their lives on the line every day to stop terrorists before they even near our borders.

In addition to the National Defense Strategy, this year we also completed the Department's first Strategy for Homeland Defense and Civil Support. Although the active, layered defense extends across the globe, this Strategy for Homeland Defense and Civil Support focuses primarily on DoD's activities in the U.S. homeland and the approaches to US territory. In those geographic layers, the Department undertakes a range of activities to secure the United States from direct attack. These generally divide into the following categories:

- **Lead:** At the direction of the President or the Secretary of Defense, the Department of Defense executes military missions that dissuade, deter, and defeat attacks upon the United States, our population, and our defense critical infrastructure;

- **Support:** At the direction of the President or the Secretary of Defense, the Department of Defense provides support to civil authorities. This support is part of a comprehensive national response to prevent and protect against terrorist incidents or recover from an attack or disaster. DoD provides support to a lead Federal agency when directed by the President or the Secretary of Defense; and
- **Enable:** The Department of Defense seeks to improve the homeland defense and homeland security contributions of our domestic and international partners and, in turn, to improve DoD capabilities by sharing expertise and technology, as appropriate, across military and civilian boundaries.

Although all combatant commands have a role to play in the active defense-in-depth of our nation, four commands – U.S. Northern Command (USNORTHCOM), the North American Aerospace Defense Command (NORAD), U.S. Pacific Command (USPACOM), and U.S. Strategic Command (USSTRATCOM) – have particularly significant responsibilities.

- USNORTHCOM, headquartered in Colorado Springs, Colorado, is responsible for planning, organizing, and executing homeland defense activities to deter, defend against, and defeat threats to the homeland and provide military support to civil authorities within its area of responsibility, which includes the continental United States, Alaska, Puerto Rico, the U.S. Virgin Islands, our territorial seas, and the coastal approaches out to 500 nautical miles. USNORTHCOM also coordinates security cooperation with Canada and Mexico.
- The commander of USNORTHCOM is also the commander of the bi-national United States-Canada North American Aerospace Defense Command. NORAD is responsible for protecting the North American

airspace over the United States and Canada. Aerospace warning and control are the cornerstones of the NORAD mission.

- USPACOM, headquartered in Honolulu, Hawaii, is responsible for the defense and support to civil authorities of Hawaii and our territories, possessions, and protectorates in the Pacific.
- USSTRATCOM, headquartered in Omaha, Nebraska, is responsible for early warning of and defense against missile attack and long-range conventional attacks, computer network defense, as well as U.S. strategic forces, military space operations, and global strategic planning. Additionally, USSTRATCOM is the lead combatant commander for integrating and synchronizing military efforts to combat WMD, including ensuring the force structure and necessary resources are in place to help all combatant commands defeat WMD.

The Department of Defense is postured to deter, defend against, and defeat threats to the United States in the air, maritime, and land domains. DoD uses the Total Force concept – the right forces for the right jobs – to execute its missions. The Total Force – Active, Reserve, and Guard – is even now engaged in activities at home and abroad that promote the security and interests of our nation. The National Guard, in particular, provides unique capabilities in every U.S. state and territory. These include: situational awareness capabilities; intelligence and information feeds; chemical-biological response force packages; and forward-deployed command and control apparatuses and joint logistics bases, as needed.

In the 20th century, DoD could largely fulfill its responsibility for protecting the nation by integrating its activities with those of the Department of State and the Intelligence Community. In the 21st century, the expertise and responsibility for managing security challenges is much more widely shared among Federal departments and agencies; State, local, and tribal authorities; the private sector; and our allies and friends abroad.

In the 21st century security environment, DoD must unify its efforts with those of its key national partners and international friends and allies to ensure the nation's security.

Defense Support of Civil Authorities

DoD has continued its long tradition of support to domestic civil authorities while maintaining its primary mission of fighting and winning the nation's wars.

There are three primary mechanisms by which DoD would take part in a Federal response to a domestic incident. Federal assistance, including assistance from DoD, would be provided: (1) at the direction of the President; (2) at the request of another Federal agency under the Economy Act, or (3) in response to a request from DHS's Federal Emergency Management Agency under the Stafford Act. The second and third mechanisms require a request for assistance and approval of the Secretary of Defense.

First, under the Constitution, the President may direct any Federal agency to provide assets in support of an incident response. The President has the authority to direct any Federal agency, with or without reimbursement, to support state and local assistance efforts in a major disaster or emergency.

Second, another Federal agency can request DoD support in accordance with the Economy Act for non-Stafford Act responses. If DoD assistance is contemplated, the requesting Federal agency submits a request for assistance through the Office of the Secretary of Defense, Executive Secretary. The request is processed through the Joint Staff and Office of the Secretary of Defense and submitted to the Secretary of Defense for a decision.

Lastly, DoD assistance may be requested under the Stafford Act. The requesting Federal agency submits a request for assistance through the Office of the Secretary of Defense, Executive Secretary. The request is processed through

the Joint Staff and Office of the Secretary of Defense and submitted to the Secretary of Defense for a decision.

Once DoD resources are employed in support of domestic civil authorities, they are under the command and control of Commander, USNORTHCOM, for responses in the Continental United States, Alaska, the Commonwealth of Puerto Rico, U.S. Virgin Islands, and the District of Columbia; or Commander, USPACOM, for Hawaii and U.S. territories, possessions, and protectorates in the Pacific region.

An important tenet of defense support of civil authorities is that DoD is always in support of domestic civil authorities. It is also important to note that the chain of command always runs from the President to the Secretary of Defense to the Combatant Commander concerned. The Department fully supports the Incident Command System of the National Incident Management System. However, at no time does the supported agency exercise any command and control over DoD forces.

Enabling Civil Authorities

In addition to providing defense support to civil authorities, DoD, recognizing that it historically has been considered a source of last resort or a source of unique capabilities, actively seeks to improve the homeland security contributions of our domestic and international partners by sharing expertise and relevant technology, as appropriate, across military and civilian boundaries. Enabling better national capabilities for homeland security missions is an important complement to DoD's homeland defense and civil support activities.

Technology is vital to the support and protection of the military now in the Global War on Terror, the transformation of the military, and to the development of capabilities for our future forces. As noted in the National Strategy for Homeland Security (July 2002), our nation's "advantage in science and

technology is a key to securing the homeland. New technologies for analysis, information sharing, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons will help prevent and minimize the damage from future terrorist attacks. Just as science has helped us defeat past enemies overseas, so too will it help us defeat the efforts of terrorists to attack our homeland and disrupt our way of life.”

Technology transfer represents an important avenue by which DoD enables civil authorities to better protect our nation and deal with the consequences of attacks. Guided by the National Strategy for Homeland Security, the National Strategy for Combating Terrorism, the Strategy for Homeland Defense and Civil Support, and other key guidance documents, DoD is helping civil authorities recognize opportunities to leverage our considerable investment in research, development, test, and evaluation to address critical homeland security technology needs.

Examples of technology transfer programs include:

- DoD assistance to the U.S Coast Guard to evaluate sensors (e.g., long-range radar systems) and platforms (unmanned aerial vehicles and high-altitude long-endurance lighter than air ships) that will enhance their ability to conduct wide area surveillance to detect, identify, and track vessels of interest;
- Numerous technologies such as ground-based sensors for the detection of humans, vehicles, nuclear material, and other contraband for use by DHS immigration, border, and customs components;
- Quadropole resonance technology developed by the Naval Research Laboratory for the Transportation Security Agency to use for cargo screening;

- Unique DoD equipment transferred to the FBI for use in response operations against threats of nuclear terrorism;
- Chemical and biological detectors to assist civil authorities in preventing the smuggling of chemical and biological WMD into the United States;
- Laser-based technologies to protect civil aircraft from man-portable air defense systems;
- Laser eye protection to shield civil aviation from ground-based lasers;
- Recent examples of technology transfer initiatives include: information-sharing systems, such as the Disaster Management Interoperability Services; biometrics identification technologies; ground sensors and their application in border security; and unmanned aerial vehicle experimentation.

In accordance with Section 1401 of Public Law 107-314 (the National Defense Authorization Act for Fiscal Year 2003), the Assistant Secretary of Defense for Homeland Defense serves as the “senior official of the Department of Defense to coordinate all Department of Defense efforts to identify, evaluate, deploy, and transfer to Federal, State, and local first responders technology items and equipment in support of homeland security.”

As part of this effort, DoD has been actively collaborating and coordinating with DHS (Science and Technology) and DOJ (National Institute of Justice). Through a series of interagency meetings, DoD facilitated the creation of a process “Blueprint” or framework for the systematic transfer of DoD technologies to the public safety community through DHS and DOJ. This framework is based, in part, on:

- DoD operating as a wholesaler while DHS and DoJ with their direct connections to and missions supporting State and local first responder networks, operating as the retailers
- The nurturing of new collaborative research, development, experimentation, test and acquisition opportunities, while avoiding duplication of effort in these areas
- Ensuring the smooth transition of appropriate missions, technologies, and capabilities to the civil sector

Having developed this initial Blueprint, DoD, DHS, and DOJ have begun a pilot of the 1401 program. In doing so, we are:

- Collaborating with the Military Services, the Under Secretary of Defense (Acquisition Technology & Logistics), Technical Support Working Group (TSWG), and Defense Logistics Agency through the 1401 Technology Transfer Working Group. The Working Group has already completed a pilot inventory of DoD technologies which resulted in several hundred items with the potential to enhance public safety. The Working Group is coordinating efforts across DoD to maintain better situational awareness of activities in support of homeland security and minimize duplicative efforts.
- Evaluating a subset of high priority technologies that with the assistance of the 1401 program could be expedited to the public safety community. DoD is working closely with DHS and DOJ in the selection and validation of these technologies, including supporting an upcoming meeting where public safety practitioners will validate and provide feedback on the selected items. The technologies include:

- An advanced sensor technology capable of real-time stand-off detection of chemical, biological, explosive, and hazardous materials (Laser Induced Breakdown Spectroscopy (LIBS))
- An improved protective suit providing chemical, biological, radiological, nuclear (CBRN), and fire protection
- An integrated system of technologies capable of providing enhanced situational awareness through improved wireless communications, real-time sharing of data and 3-D positional information for communication in buildings and tunnels
- Collecting and documenting the successful transfer of technologies to the public safety community. We are continually working within DoD as well as with DHS and DOJ to identify current and ongoing collaborative efforts focused on improving homeland defense and homeland security.

Over the next few months, we will continue to develop and refine the 1401 process and expand outreach activities to first responders. Upcoming activities include:

- Conclusion of the pilot implementation of the 1401 process Blueprint including the documentation of lessons learned and generation of process improvement recommendations
- Execution of a Memorandum of Agreement (MOA) with DHS and DOJ which outlines roles and responsibilities as part of the 1401 process. It is expected to be ready for signature in the Fall of 2005.
- Sponsorship of the annual *Technologies for Critical Incident Preparedness Conference and Exposition* in San Diego, CA. We will also be showcasing several DoD technologies applicable to homeland security.

- Continue outreach activities and collaboration with Non-governmental organizations focused on technology transfer, including Congressionally-directed work at the Institute for Entrepreneurial Excellence (“FirstLink”) at the University of Pittsburgh and DoD’s TechMatch program (part of the West Virginia High Tech Consortium).

In compliance with Section 1401, DoD will continue its efforts to transfer competencies between DoD and the civil sector—through technology transfer and sharing DoD’s “lessons learned” from applicable exercises and program management.

Such collaboration can increase the overall effectiveness of national capabilities and potentially reduce other agencies’ dependencies on limited DoD assets.

Examples of other technology transfer programs under the auspices of 1401 include:

- The Defense Logistics Agency (DLA) 1033 program, which provides over 17,000 Federal, State, and local law enforcement agencies with excess DoD counter-drug and counterterrorism equipment;
- The Army administered 1122 program, which allows State and local governments to participate in U.S. Government purchases of law enforcement equipment suitable for counter-drug activities and, therefore, realize significant discounts due to the large volumes involved.
- The Disaster Management Interoperability Service (DMIS), a first responder information sharing and collaboration tool originally developed by the U.S. Marine Corps and transferred to the Federal

Emergency Management Agency. Recognized as a Presidential e-gov initiative, DMIS is installed in every state, has over 34,000 registered users, and is used for over 70 incidents per month.

- A hazardous materials (HAZMAT) bags that emergency responders can use to safely transport WMD devices;
- Radiological decontamination technologies to identify, quantify, and reduce the radioactive contamination in the aftermath of a WMD incident;
- A foam-based decontamination system that has broad effectiveness against chemical agents; and
- The interagency Technical Support Working Group (TSWG), a U.S. national forum that brings together over 85 Federal agencies to identify, prioritize, and coordinate interagency and international research and development requirements for combating terrorism. DoD provides the bulk of funding for the TSWG (e.g., \$94M of the FY04 \$165M budget). These technologies typically are also applicable to first responders and other homeland security missions, such as:
 - An electrostatic decontamination system;
 - A next generation firefighter protective ensemble;
 - A small, self contained gamma ray and thermal neutron radiation detector for use in the detection and presence and location of radioactive materials; and
 - An emergency responders' decision support system, which contains information on responses to large improvised explosive devices, toxic industrial chemicals, chemical

warfare agents, and biological agents likely to be employed by terrorists.

Conclusion

Throughout our history, U.S. military forces – Active Duty, Reserves, and National Guard -- have defended our nation against its enemies on land, at sea, and in the air, adapting continuously to engage threats to our nation. Today we must cope not only with the threats produced by the proliferation of weapons of mass destruction and missile technology among nation-states, but also with threats posed by individual terrorists and terrorist networks with global reach.

Chairman Saxton, Representative Meehan, Chairman Cox, Representative Thompson, distinguished members: thank you for your interest in, and support of, the Department's homeland defense mission and how the Department can best enable civil authorities to better secure our nation. The citizens of this nation, its institutions, and our brave men and women in uniform have repeatedly demonstrated the patriotism, innovation, determination, and resiliency to defeat our enemies while retaining our freedoms. There is no doubt in my mind that those capabilities will be tested against this newest enemy threat – nor is there any doubt that we will prevail.