AAAS Science and Security Workshop
July 13, 2004

John Marburger
Director, Office of Science and Technology Policy
Executive Office of the President

Thank you for inviting me to speak today. Much of interest to the national security community has transpired during the thirty-four months since the terrorist attacks of 9/11, and I thought it would be useful today to review a select list of science and technology responses to the threat of terrorism. I am going to use as my guide the 2002 National Academies study *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Probably everyone here is familiar with this report, one of the most useful among many that appeared after the terrorist attacks of 9/11.

Making the Nation Safer addressed nine critical areas:

Nuclear and Radiological Threats;   Human and Agricultural Health Systems;
Toxic Chemicals and Explosive Materials;   Information Technology;
Energy Systems;   Transportation Systems;
Cities and Fixed Infrastructure;   The Response of People to Terrorism; and
Complex and Interdependent Systems.

Each area has seen significant organizational and jurisdictional changes, most notably through the creation of the Department of Homeland Security (DHS). My plan is to highlight a few government programs that have been implemented within each area, and conclude with some remarks on mechanisms of coordination and policy creation. In most cases, I will be able to tell you how funds requested for the fiscal year (FY05) that begins in October will be used to enhance activities in these areas.

Nuclear and Radiological Threats

The Administration is pursuing a multi-tiered approach to prevent and mitigate the terrorist use of a radiological or nuclear device within the United States.
- improve security of special nuclear materials in other countries.
- enhance international nuclear counter-proliferation efforts.
- develop better passive and active detection technologies to locate and interdict nuclear or radiological material before it can enter the country.
- fund R&D to improve crisis response (*e.g.* advanced search, render safe).
- enhance consequence management including remediation and medical triage.

The Department of Homeland Security has the lead on enhancing border security and detection of nuclear and/or radiological material internal to the United States. Some specific DHS initiatives include:

- *Systems Architectures and Pilot Deployments* – DHS is establishing test beds to prevent nuclear or radiological material from entering cities. One, for example, is in cooperation with the Port Authority of New York and New Jersey. Radiation detection equipment is being installed at tunnels, bridges, ports and airports in the New York City metropolitan area, and all functions associated with their operational use will be evaluated.
- *Technology Development Initiatives* – Development of detection standards, passive radiation detection and active interrogation technologies for the detection of special nuclear materials, nuclear weapons assemblies and radiological threats.
- *Incident Management* – Development of technologies and training aids for use in the aftermath of an event (consequence management) to facilitate situational awareness, clean up, and medical triage. DHS established the Nuclear Assessment Program to provide inspectors with the capability to obtain secondary "reach back" support that can be used to resolve radiation detection alarms at inspection locations.
- *Pre-Planned Product Improvements* – Rapidly develop and transition enhanced capability to deployed detectors/systems. Rapidly incorporate advances in prototype technologies into commercial offerings of rad/nuc detectors/systems for use in operations.

Human and Agricultural Health Systems

For nearly a year, DHS has deployed continuously operating biological pathogen detection systems to approximately 30 U.S. cities as part of the *BioWatch* program. FY2005 budget requests would improve biosurveillance activities in the Department's Information Analysis and Infrastructure Protection (IAIP) and the Science and Technology (S&T) Directorates. $65 million has been requested for S&T to enhance current environmental monitoring activities, bringing the total to $118 million. In IAIP, $11 million is requested to integrate, in real-time, biosurveillance data collected from the nationwide network with information from health and agricultural surveillance and other terrorist threat information from law enforcement and intelligence communities.

During the current fiscal year (FY04) approximately $3.8 billion went to the Department of Health and Human Services to fund biodefense research. Part will go toward improving state and local health systems and their ability to cooperate with federal efforts during a bioterrorism emergency. Next year's budget (FY05) includes $1.75 billion for biodefense research at NIH. Within that total is $150 million for the construction of biosafety laboratories for NIH to help develop medical protection from bioterrorism, and to back up State and Federal public health labs. Prior to 2002, only a few laboratories in the U.S. were capable of working with bio-terrorism agents. The new funds will provide an additional 20 biosafety level 3 labs throughout the country. Research objectives for the new funding include vaccines, diagnostic tests for first responders, and therapies for biopathogens likely to be used by terrorists.

The *National Biodefense Analysis and Countermeasures Center* (NBACC), a center of the Department of Homeland Security's Science and Technology Directorate, provides scientific support for intelligence activities, prioritized biothreats, and also conducts bioforensics analyses contributing to attribution and hence to deterrence. The NBACC, located on the Fort Detrick, Md. campus, will support public and agricultural health, law enforcement, and national and homeland security by providing hub laboratory capabilities.

Toxic Chemicals and Explosive Materials

In cooperation with the National Institute of Standards and Technology (NIST) and the Office of Law Enforcement Standards, the DHS S&T Directorate has adopted a set of standards for personal protective equipment for first responders against chemical, biological, radiological, and nuclear incidents. These standards are intended to assist state and local officials and manufacturers in providing emergency gear.

A Water Security Research and Technical Support Action Plan is being developed by EPA's National Homeland Security Research Center within the EPA Office of Research and Development. The Plan is directed toward protection of the nation's water supplies and distribution systems from terrorist attacks. Primary emphasis is on water supply, treatment, and distribution infrastructure, with research on detection and characterization of contaminants, response and mitigation, and prevention and protection.

Information Technology

DHS has requested $18 million in FY05 to enhance cyber security research emphasizing
- leveraging private sector activities,
- public-private partnerships,
- "non-technology" aspects,
- policy and leadership to help drive changes.

This research is in addition to the cyber security work at NSF, DoD, and NIST in areas such as trusted operating systems, robust authentication, and protection against malicious code or insiders.

This year (FY04) the DHS Threat Vulnerability, Testing and Assessment unit co-funded the Cyber Defense Technology Experimental Research Network (DETER) with the National Science Foundation. This $5.45 million, three year, multi-university research project will be led by the University of California at Berkeley to create an experimental infrastructure network to support development and demonstration of next-generation information security technologies for cyber-defense.

The DHS S&T Directorate is responsible for the management of Project SAFECOM, a Presidential E-Government initiative for coordinating Federal wireless interoperability activities. SAFECOM's mission is to enable public safety operations nationwide -- including local, tribal, State and Federal operations -- to be conducted with

full and efficient inter-communication. Guidelines for interoperable communications gear have been published and common grant guidance has been developed and incorporated into the public safety wireless interoperability grant programs of both the Department of Justice and the DHS.

Energy Systems

DHS has overall responsibility for a list of 14 critical infrastructure sectors and key assets. The S&T Directorate is working with DOE and the Electric Power Research Institute (EPRI) to develop mutually beneficial security R&D programs. Among several other areas, DHS is focused on SCADA (supervisory control and data acquisition) systems. DHS is also working with industry and technical standards groups to identify needs and best practices. Recently DHS delivered a prototype system to perform Geographic Information System (GIS) based computer assisted threat and vulnerability mapping of the oil and gas infrastructure in the Southwestern United States.

Transportation Systems

The DHS S&T Directorate has a Counter-MANPADS program to identify, develop, and test a cost-effective means to protect commercial aircraft against the threat of man-portable anti-aircraft missiles. This program also addresses the science and technology base needed to reduce the vulnerability of commercial aircraft to terrorist attack using these portable weapons.

The President's FY05 budget request includes $24 million for personnel and operations dedicated to security in non-aviation transportation modes, and $17 million to support the Transportation Security Administration's around-the-clock Transportation Security Coordination Center (same funding as FY04). The complex, interdependent land transportation environment is especially challenging. TSA will continue to assess the risk of terrorist attacks to non-aviation transportation, assess the need for standards and procedures, and ensure compliance with existing regulations.

Cities and Fixed Infrastructure

The Safe Cities Program, supported by DHS, is a pilot program currently running in select cities. It implements technology and operational systems in cooperation with state and local emergency managers and city planners, and identifies needs and gaps that might be met with advanced technologies under development with DHS and other agency sponsorship.

A hazard assessment tool for security management at large events, such as bowl games and conventions, has been developed for use by event managers. Called LINC, for Local Integration of (National Atmospheric Release Advisory Center -- NARAC) with Cities, this tool provides local governments with advanced operational atmospheric plume prediction capabilities. In the event of a chemical or biological release, NARAC predictions can be used by emergency managers and responders to map the extent and

effects of hazardous airborne material and determine protective strategies. New York City used LINC to help inform and manage an explosion and fire at a Staten Island refinery last year.

Project *PROTECT* (Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism) is a team effort between the Department of Homeland Security, the National Laboratories, the Washington Area Metropolitan Transit Authority and the First Responder community in Montgomery County, MD; Arlington, VA; and the District of Columbia. This is an operational chemical agent detection and response capability, currently deployed at Metro stations and operated by the WMATA. The system integrates chemical detector data and video feed and transmits the integrated information to the Operations Control Center (OCC) where the information is analyzed and an event confirmed. The information is then transmitted to the first responders who access it both in their OCC and through the use of wired jacks on the scene to facilitate response and recovery. PROTECT can be applied to other areas such as fire and emergency response, security and forensics. Other federal partners include the Federal Transit Administration, the Department of Transportation, and the National Institute of Justice. Several private industry partners have also contributed significantly to this process.

The Response of People to Terrorism

The Homeland Security Center for Risk and Economic Analysis of Terrorism Events (HS-CREATE) came into existence last November to address both the targets and means of terrorism. This is a multi-university collaboration in which the University of Southern California has the lead, and includes the University of Wisconsin, New York University, Berkeley, RPI, and Cornell. The emphasis is on protecting critical infrastructure systems such as electrical power, transportation, and telecommunications. It also studies tools for communicating risk in ways that elicit appropriate responses from individuals, families, organizations, *etc.* in the event of an attack. DHS will provide the consortium with $12 million over the next three years for the study of risk analysis related to the economic consequences of terrorist threats and events. DHS is planning other HS Centers across a spectrum of short and long range R&D areas.

Complex and Interdependent Systems

DHS's Threat Vulnerability, Testing and Assessment program developed and has installed the Threat Vulnerability Mapper (TVM) as part of DHS's Threat and Vulnerability Integration System. The TVM provides counterterrorism analysis in a user friendly format, depicting the geographical distribution of threats across the country, and searching underlying databases for information on possible actors, agents, potential severity of attacks and extent of vulnerabilities to and effects of such attacks. I have not seen this system in operation, but it could obviously serve as a central tool for event management as well as analysis.

As an example of a real ability to respond, last December, DHS's Critical Infrastructure Decision Support System was asked to conduct a rapid analysis of potential consequences following the discovery of a cow in Washington State with bovine spongiform encephalopathy (BSE) or Mad Cow disease. An analysis was developed within hours using available open literature, past historical data, and the results from an early state dynamic simulation agriculture model.

You can see there is a lot of action -- and a lot of new acronyms and operations within the Department of Homeland Security. There is also an impressive amount of interagency and intergovernmental cooperation in every one of the nine areas of the National Academy Report. Recall that the current system has its origins in the Office of Homeland Security (OHS) established shortly after 9/11 in the White House. My office (OSTP) provided technical support, not only in policy but also in operations, to OHS until Congress created the new Department of Homeland Security in March 2003. At that time, the old OHS was converted to the Homeland Security Council, a parallel organization to the National Security Council, and all operational responsibility passed to DHS. Today OSTP coordinates interagency homeland security science and technology, with DHS as a lead agency. This coordination is accomplished under committees and working groups of the National Science and Technology Council.

These concrete examples of technological aspects of the nation's counter-terrorism activities give you an idea of the scope and level of detail of the work being done. We have a lot more to do, but I am convinced we are not only better prepared to defend ourselves against terrorism today, but our national civil infrastructure is getting some long overdue improvements as a result of this attention to homeland security.

I would be glad to discuss any of this material further in response to your questions.