

Statement for the Record

**The Honorable Jay Cohen
Under Secretary for Science & Technology
Department of Homeland Security**

**Gregory Giddens
Director, Secure Border Initiative Program Executive Office**

Department of Homeland Security

**Before the U.S. House of Representatives
Committee on Science**

September 13, 2006

Introduction

Good morning. Chairman Boehlert, Congressman Gordon, and distinguished Members of the Committee, it is a pleasure to be with you today to discuss the progress the Department of Homeland Security is making in the nation's efforts to secure America's borders. Today, in accordance with the Committee's letter of invitation to testify, we will focus our testimony on how technology can help secure our borders, especially the ways in which science and technology support the Department of Homeland Security's Secure Border Initiative.

Under the Secure Border Initiative, the Science and Technology (S&T) Directorate supports the homeland security missions of U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), Intelligence and Analysis (I&A), US-VISIT, the Domestic Nuclear Detection Office (DNDO), and others by conducting, stimulating, and enabling research, development, test, evaluation, and timely transition of homeland security capabilities to end-users in the field.

Problem Statement

The challenge of securing the nation's borders is enormous. Border security is a continuum that begins far beyond the borders of the United States and continues to the interior of our country. It involves the movement of both people and goods and is not successful unless it protects the country from harm and allows lawful trade and immigration. Border security requires a critical blend of tangible resources such as equipment and personnel, along with intangible items such as useful intelligence and strong partnerships with foreign governments. Securing the United States borders is a Presidential priority. In his May 15, 2006, Address to the Nation, President Bush said, "First, the United States must secure its borders. This is a basic responsibility of a sovereign nation. It is also an urgent requirement of our national security. Our objective is straightforward: The border should be open to trade and lawful immigration -- and shut to illegal immigrants, as well as criminals, drug dealers, and terrorists. ... We are launching the most technologically advanced border security initiative in American history. We will construct high-tech fences in urban corridors, and build new patrol roads and barriers in rural areas. We will employ motion sensors, infrared cameras, and unmanned aerial vehicles to prevent illegal crossings. America has the best technology in the world, and we will ensure that the Border Patrol has the technology they need to do their job and secure our border."

To date, much of the work of S&T has been focused on the actual border, both at ports of entry and between ports of entry. The current technologies being used between ports of entry to secure the border include cameras and Unattended Ground Sensors (UGS) to detect and identify illegal border intrusions. Cameras - both daylight and thermal infrared that are installed on poles and other structures along high-volume illegal alien traffic areas of the border - constitute the Remote Video Surveillance (RVS) system. UGS are also used along high-volume illegal alien traffic areas of the border.

The current systems provide a remote detection and identification capability, but with limitations. For example, (1) sensors are not able to differentiate between illegal activity and

legitimate events; (2) RVS cameras cannot automatically detect any activity or movement and are limited by weather; (3) sensors are limited by battery power and RVS cameras have infrastructure requirements; and (4) system effectiveness is dependent upon the availability and capability of skilled operations and maintenance personnel.

Secure Border Initiative

The Secure Border Initiative (SBI) is the Department's approach to lead, integrate, and unify our efforts against cross border and international activities that threaten border security. SBI's approach is that the border is not merely a physical frontier and effectively securing it requires attention to processes that begin far outside the US borders, occur at the border and continue to all regions of the United States. SBI brings a systems approach to meeting this challenge; its mission is to integrate and unify the systems, programs and policies needed to secure the border and enforce our customs and immigration laws. It is a national effort to transform the border security continuum with the objective to disrupt, dismantle and deter all cross-border crime and balance legitimate travel and trade into and out of the United States.

The Science & Technology Directorate is supporting SBI by providing the systems engineering tools, processes, and manpower to ensure that SBI implementation is effective and affordable. In addition to providing systems integration, analysis and engineering support, S&T is developing an integrated systems model. Using modeling & simulation, SBI decision makers will have the tools to make informed choices for investment strategies and program and policy formulation. The decision makers will understand: 1) where to invest scarce resources (e.g., how many agents and detention beds, how much technology and fencing), 2) the trade-offs associated with their decisions, and 3) where the gaps and risks are. The first phase of this model focuses on the immigration system.

Technology is required that will provide better detection of illegal activity and situational awareness to give us the ability to make near-real-time strategic and tactical decisions regarding our response. These technological capabilities will include new sensors and platforms using manned, unmanned, ground, air, maritime or perhaps even space assets, as well as command and control, decision support aids, robust communications capability, surveillance equipment, and data transfer.

DHS has a requirement for a Common Operating Picture (COP) at the tactical, operational and strategic levels that can seamlessly interface with systems used by other federal, state and local law enforcement partners. Better situational awareness and command and control at the border will facilitate the apprehension and location of individuals and groups who have violated or intend to violate the border. Leveraging emerging technologies and the development of standards, protocols and symbology enables the creation of common user views and information exchange. These common views and information then may be shared with all who operate at the border, independent of the method an agency chooses to implement its specific COP.

S&T is also developing and transitioning technologies critical to *SBI_{net}* (a component program of SBI) per the request of CBP, which is the executive agent for this program. Specific needs to be addressed to enhance the ability to detect and interdict illegal border activity are:

- Improved technology for detection, classification and interdiction of illegal activity and enhancing the ability to make rapid strategic and tactical response decisions.
- A COP of the border environment for tactical and operational planning with other federal, state and local law enforcement partners.
- Access by DHS personnel, both at and between ports of entry, to the same information at the same time to ensure tight coordination and effective response to all threats.
- Rapid response capabilities to effectively respond to cross-border violations, including technologies that improve situational awareness, command & control, and communications, and provide decision aids for commanders.
- Identification of individuals with hostile intentions toward the United States and its citizenry and secure and accurate communication of that information to those who can expeditiously assess the risk of each person, leading to timely interdiction.
- Technologies that aid in the deterrence and channeling of illegal cross-border activity.
- Technologies that survive rugged handling and extreme environmental and operational conditions with improved reliability and maintainability.
- Technologies that improve voice and data connectivity in remote field areas.

While SBI initially focuses on land border security, it will also address security of the U.S. maritime borders. Specific needs to be addressed to enhance maritime border security are:

- Improved detection, surveillance and reconnaissance capabilities in ports and off shore, using improved platforms, communication networks, and sensors; as well as vessel tracking and anomaly detection

The goal is to provide agents and officers with a total scene awareness capability that provides a geo-spatially referenced detection, classification and tracking capability along with collaboration and decision making tools to improve efficiency. Only highly reliable technologies, coupled with a validated and improved concept of operations, will meet the goal. Greater confidence in successful interdiction through advanced technology will lead to force efficiencies and an enhanced ability to prioritize the deployment of intelligence, surveillance, and reconnaissance assets. The effectiveness of any one technology must be balanced against the considerations of its impact on ancillary systems including people, processes, and other deployed technologies.

While SBI is a multi-year development, it looks to S&T to provide technology insertion on a 12-18 month cycle. This insertion into SBI will be in the form of system hardware specifications, software code, supporting documentation, and lessons learned from technology developments and operational tests.

Risk

As stated above, the President has declared that securing our borders is an urgent priority for the national security. Not resolving existing capability gaps directly impacts the Department's overall mission to prevent and deter terrorist attacks. One of the Department's highest priorities

is the prevention of the entry of terrorists and their instruments of terror into the United States. S&T addresses this priority by providing technology and processes for detecting, apprehending and prosecuting this illegal activity.

S&T conducts continuing technical evaluation of current and future risks to the borders as a foundation of risk-based decision-making by both the S&T Directorate and the Department of Homeland Security. Additionally, S&T analyzes and distills scientific and operational information to better inform strategic and operational choices made by decision-makers. S&T also conducts technology evaluation and assessment by identifying, developing, testing, and facilitating the transition of advanced homeland security technical capabilities to DHS's operational components and state, local and tribal entities.

S&T also reduces risk by prototyping concepts and technologies and demonstrating their capabilities in an operational environment. We are currently piloting two important capabilities that we call BorderNet and COP/Data Fusion System at the Douglas Border Patrol Station in the Tucson Sector. These systems are force multipliers that decrease officer workload and response time and increase detection and apprehension of illegal border crossers. The results from our prototyping and pilots provide valuable lessons learned for SBI and future systems development. This approach ensures that the most advanced technological solutions are provided to those who protect our borders and that new capabilities are deployed to the field in the shortest possible time and at an affordable cost.

S&T Border Security Programs

The Department of Homeland Security has already put several new technologies in place to aid in securing our borders. Besides BorderNet and the COP/Data Fusion System, we have provided a long range acoustic device (LRAD), which gives Border Patrol agents the ability to communicate with persons at a long distance and we partnered with CBP in deploying Unmanned Aerial Vehicles along the Southern border. We continue to develop and demonstrate new and enhanced capabilities to ensure enhanced security.

The Border Watch Program is a technology-based initiative to develop and transition capabilities that improve the security of our nation's borders. Its goal is to develop and integrate information management and sensor technologies necessary to prevent the entry of terrorists and their instruments of terror, criminals, and illegal aliens through our nation's borders. Border Watch technologies will be integrated into SBI as capabilities mature. Border Watch consists of the following program components:

- Border Detection Grid,
- Border Network (BorderNet),
- Border Protection Pattern Discovery and Prediction, and
- Common Operating Picture (COP).

The Border Detection Grid components will identify available sensors and sensor monitoring capabilities, as well as technology gaps, in order to achieve persistent electronic surveillance of the U.S./Mexico and U.S./Canada borders. The detection target includes people or groups of

people on foot, in vehicles (cars, trucks, and snowmobiles), and in tunnels, vessels, and low-flying aircraft. Sensor and sensor platform technology gaps will be addressed through studies, system design and development, test and evaluation, and/or pilot programs. The program will investigate the potential use of radar, Electro-Optic/Infrared (EO/IR) cameras, unattended ground sensors (UGS), fiber optic tripwires, and other emergent sensors. Sensor platforms will include fixed and mobile towers, vehicles, and manned and unmanned airborne vehicles. Variations in environmental conditions (terrain, weather, marine versus land) and communication availability are expected to drive the solution set for different geographical areas. Department of Defense sensors and sensor systems will be surveyed and adopted, as appropriate.

The Border Network (BorderNet) is a proof-of-concept, prototype development. Capabilities will be developed in spirals with each spiral providing greater capability and user base. BorderNet provides Border Patrol agents with the capability to conduct biometric and biographic queries to identify detainees, in the field and at the time of apprehension. Fusion of multiple data sources provides the agent with actionable intelligence in the form of indications, warning and incident responses recommendations. BorderNet also generates a tactical situation awareness display at the agent and station level, and includes sensor alerts and blue force tracking (BFT) or friendly force ID. Target tracks generated by the COP/Data Fusion System, developed under the Arizona Border Control Initiative, provide overlays on the BorderNet situation awareness display. Field agent connectivity to the various information sources occurs via wireless communications using handheld digital devices and vehicle mounted mobile data computers. Initially, BorderNet accesses biographical data from the Enforcement Case Management System (ENFORCE), the Automated Biometric Identification System (IDENT), and the National Criminal Information Center (NCIC) based on personal data collected from a detainee. NCIC will be accessed through the Arizona Criminal Justice Information Center. Vehicle registration and status information will be obtained through the Arizona Department of Public Safety. Subsequent spirals will connect to the Homeland Security Information Network (HSIN) and the Homeland Security Data Network (HSDN), as well as other local, state and national data sources. Additional features in future spirals may include language translation, knowledge discovery, improved Blue Force Tracking, detainee field enrollment, video transmission, detainee tracking, federated query, and northern border applications.

Border Protection Pattern Discovery and Prediction technologies will provide a new capability to Customs and Border Protection to rapidly fuse disparate information sources to discover geo-spatial, behavioral, and temporal patterns and indicators that provide field agents local scene awareness and actionable intelligence. A prototype will be developed in concert with CBP customers, which will develop patterns and indicators that address topics such as:

- 1) crossing routes and staging areas for cross border smuggling,
- 2) crossing patterns by group – to discover patterns that will help identify the number of organized groups involved and their respective "signatures,"
- 3) crossing patterns by tactic – to discover patterns that will help identify distinctive "signatures" for specific tactics, such as drug smuggling, human smuggling, etc.,
- 4) identifying the links and patterns between illegal border crossing and criminal activity within the U.S., and

5) tunnel activity – to discover the likely next tunneling start and end points.

The Common Operating Picture (COP) component will provide the capability to fuse and display at a tactical level the information from select assets within DHS, including but not limited to, Border Patrol Stations, Ports of Entry (POE) and the U.S. Coast Guard. It will be a layered architecture, scalable from the agent/officer in the field to the DHS Operations Center. It will use multi-level security and authentication measures to protect sensitive information and will provide collaborative tools as decision aids. It will use an approved set of standards, including interfaces, services, protocols, and supporting structures. The COP will provide a command and control capability and a tool for inter-agency collaboration. Initially, it will be a sector capability focusing on the southwest border. Subsequent versions will expand to include additional DHS components.

Unmanned Aerial Vehicles (UAVs)

The Department of Homeland Security has made a great deal of progress in the area of UAVs over the past three years. At the request of Congress, S&T led an extensive study effort, involving all DHS operational Components, Department of Defense (DoD), Department of Transportation (DoT), Federal Aviation Administration (FAA), and National Aeronautics and Space Administration (NASA) that provided a comprehensive evaluation on the uses of UAVs to support DHS missions. The report was delivered to Congress on time on March 31, 2004, as directed.

Beginning in the summer of 2004, S&T funded two major UAV evaluations as part of DHS' Arizona Border Control Initiative (ABCI). The first period of operational evaluation ran from June through September and utilized the Hermes 450 UAV. The second period of operational evaluation employed the Army's Hunter UAV with operations beginning in November 2004 and continuing through January 2005. The data from these evaluations and other analyses, including an extensive Analysis of Alternatives developed by S&T, led to the establishment of a DHS UAV initial operational capability along the Southern Border.

S&T worked very closely with CBP to acquire DHS's first UAVs to support the initial operational along the Southern Border. The initial DHS/CBP UAV capability, consisting of one UAV system (1 aircraft and ground control equipment), became operational in 2005. CBP is the lead for operations and acquisition with S&T providing program and systems integration support. The priority for DHS/CBP UAVs will be to support CBP operations along the border but they will also be used by S&T for evaluation and development of new UAV payloads and systems that will continuously improve DHS UAV mission effectiveness.

Current FAA restrictions on the use of UAVs within United States air space limit their utilization. S&T is working with DoD and FAA to remove current flight restrictions on Border Patrol Southwest border operations through the development of Sense-and-Avoid capability to allow freer use of CBP UAVs in the national air space.

Conclusion

The Department of Homeland Security believes strongly that, only by developing the border security technologies that will be needed five and ten years from now, can we fully ensure that the nation will be secure for decades to come.

Mr. Chairman, Congressman Gordon, and Members of the Committee, this concludes our prepared statement. With the Committee's permission, we request our formal statement be submitted for the record.

We thank you for the opportunity to appear before this committee and we will be happy to answer any questions you may have.