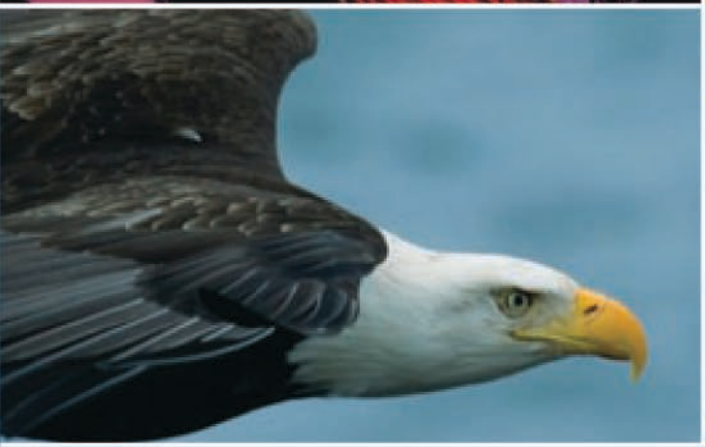


Science and Technology for a Safer Nation

Homeland Security

Science and Technology

March 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Science and Technology for a Safer Nation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Homeland Security,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**41**	

FOR THE TRANSPORTATION SECURITY ADMINISTRATION

- **Home Made Explosives** signature data that informed the decision to allow air travelers to carry small quantities of liquids
- **Screening Passenger by Observation Techniques** analysis that delivers enhanced capabilities in detecting suspicious behavior through cross-culturally validated observational and interview techniques that can be employed well before a person commits a hostile act
- **Behavior-Based Deception-Detection Training** enables cross-cultural validation of behavioral indicators of deception and suspicious behavior
- **Hand-Held Vapor-Detection** technology to detect and identify persistent but low-vapor pressure chemical threats on surfaces

FOR OTHER U.S. GOVERNMENT AGENCIES

- The **National Bioforensics Analysis Center** that conducts forensic analysis of evidence from biocrime or bioterrorism events
- High-throughput **integrated mobile laboratories** for broad-based tactical chemical analysis
- Material threat determinations to inform Health and Human Service's medical countermeasure requirements generation
- End-to-end **BioTerrorism Risk Assessment, Chemical Terrorism Risk Assessment** and integrated **CBRNE Risk Assessment** capabilities to assess cross-threat risks and evaluate risk-mitigation strategies
- The **Biodefense Knowledge Center** that provides tailored, in-depth biodefense analysis and "24/7" operational support
- The **Chemical Security Analysis Center** that analyses current and evolving chemical threats and provides "24/7" technical reach-back support
- The **Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks** tool that provides automated analysis of possible attack paths through a cyber network for attack correlation, prediction and response
- A **secure USB device** that corrects a significant cyber-security vulnerability

FOR STATE AND LOCAL FIRST-RESPONDERS

- A man-portable **Interoperable Tactical Operations Center**
- The **critical infrastructure inspection** management system that enables officers to locate quickly and inspect critical infrastructure
- Seven **hurricane scenario models** for New York City restoration planning
- Guidance for **critical transportation facilities** following a biological incident
- A networked **chemical detection system** for rail transportation facilities
- A nationwide **validation and testing program for communications equipment** to ensure interoperability

FOR EVERY ONE

- A **Global Terrorism Database** containing more than 85,000 events to analyze and understand factors that influence the likelihood of a terrorist attack

ONE :: PERSPECTIVE

PERSPECTIVE :: 1
- Science and Technology for a Safer Nation
- Threats and Challenges
- Strategic Goals and Objectives
- The Way Forward

FRAMEWORK FOR S&T SUCCESS :: 6
- Pushing S&T Envelopes
- Requirements to Reality
- Measuring Our Success
- A Global Perspective

AN "ALL HANDS" EVOLUTION :: 12
- The Human "Element"
- Techsolutions
- Science and Technology Advisory Committee
- Interagency Outreach
- International Collaboration
- Analysis and Experimentation
- Special Programs
- Test & Evaluation/Standards
- Office of National Labs
- University Programs

DELIVERING RESULTS :: 27
- Explosives
- Chemical and Biological Threats
- Command, Control and Interoperability
- Borders and Maritime Security
- Human Factors
- Infrastructure and Geophysical

A FUTURE OF HOPE & SECURITY :: 40

SCIENCE AND TECHNOLOGY FOR A SAFER NATION

Advanced technologies and systems in the hands of dedicated people throughout the United States are the nation's asymmetrical advantages in safeguarding our security. U.S. leadership in science and technology is vital to the security of the homeland as well as the safety of our allies, coalition partners and friends worldwide. "Now, more than ever," then-Secretary of State Colin Powell remarked in 2004, "American science must enlighten American statecraft." This fundamental perspective guides the strategies, plans and programs of the Science and Technology (S&T) Directorate in the Department of Homeland Security.

The Homeland Security Act of 2002—which established the Department of Homeland Security (DHS)—requires that the Department plan, coordinate and integrate all U.S. government activities relating to homeland security, including border security, intelligence, critical infrastructure protection, emergency preparedness and response, and science and technology. Underscoring the critical role of science and technology to America's security, the Act gave the Science and Technology Directorate the responsibility to advise the DHS Secretary on S&T requirements, priorities and programs that support the Department's vision and mission.

The 2002 Act also charged the S&T Directorate to carry out basic and applied Research, Development, Test and Evaluation (RDT&E) for America's homeland security needs. And, among other initiatives and mandates, the Act called for a specialized Homeland Security Advanced Research Projects Agency (HSARPA, patterned after the Defense Advanced Research Projects Agency) within the S&T Directorate to:

...support basic and applied homeland security research to promote revolutionary changes in technologies; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.

Continued U.S. leadership in science and technology is essential in the war on terrorism in all its forms. Homeland security teams must also deal with all hazards and all risks, including hurricanes, floods, forest fires and earthquakes. When the next terrorist attack or disaster comes, the nation's security professionals and first responders must be up to the task.

THREATS AND CHALLENGES

Significant and varied challenges confront us. People, weapons or diseases that would do us harm can enter the U.S. homeland at many points along our more than 95,000 miles of coastlines and 6,000 miles of land borders, as well as through more than 360 ports and almost 20,000 commercial airports, general-aviation facilities and private airfields from Maine to Guam. The United States must have a global perspective and technological edge that will enable us to address a broadest spectrum of threats. Dealing with external threats is made much more complex by the "home-grown" danger from terrorists and extremist groups operating within the United States, as well as the challenge of readying for, and responding to, natural and man-made disasters that require federal assistance.

The Prussian monarch Frederick the Great long ago warned, "He who defends everything, defends nothing." That is as true today as it was in the 18th Century. We continue to assess and reassess vulnerabilities, potentials for harm, probabilities of occurrence and likelihoods of location. From such informed risk assessments, we craft the strategies, doctrines, programs and tactics that span law-enforcement, homeland-security and -defense and natural-disaster requirements and operations. Our highest priority is to develop help technologies and systems that will enable DHS operational components and first responders to deal with dangers to America's safety and security.

A Broad Spectrum of Dangers

- :: Chemical, Biological, Radiological, Nuclear and Explosive-enhanced (CBRNE)
- :: Weapons of Mass Effect (WMEs)
- :: Improvised Explosive Devices (IEDs) that can be placed in cities and towns,key infrastructure, ports and waterways
- :: "Cyber-attacks" against our financial, industrial and governmental information networks
- :: Suicide bombers in aircraft, vehicles, ships and small craft
- :: Smuggling of drugs, weapons and people
- :: Global diseases
- :: Environmental attacks
- :: Political and religious extremism
- :: Mass migration flows
- :: Man-made and natural disasters

Among the multi-dimensional array of threats and challenges that confront the United States in 2008 are three areas of increasing concern.

First is the need for seamless connectivity and interoperability among communications and information-sharing systems that virtually link all levels of support—from the White House to first responders. Recent natural and man-made events underscore strategic, operational and tactical impediments we face from a lack of interoperability in the nation's command, control and communications systems and communications protocols and architectures. Lack of communications interoperability can hamstring situational awareness, command and control and response efforts, however heroic.

Second is the threat of improvised explosive devices (IEDs). The specter of makeshift but lethal homemade explosives and Weapons of Mass Effect in America's gathering places, streets, subways, highways and railways threatens indiscriminate victims and could cause intense fear and significant economic and political impacts. Deployed surreptitiously underwater or delivered by suicide boats, IEDs in our ports and waterways could have chilling effects on the nation's trade—more than 90 percent of which is carried by ship and is critical for our globalized just-in-time and just-enough economy. Response to a domestic IED threat will be completely different from what U.S. forces handle overseas, as there are law-enforcement and infrastructure-protection concerns here that do not figure in military operations. We must focus on prediction and move our deter-to-detect-to-respond-to-recover efforts months and miles away from an actual attack. If we get the bomber, we do not have to worry about the bomb's effects. For these compelling reasons, in Fiscal Year (FY) 2008 we put in place a Counter-IED/Counter-Vehicle Borne IED special project that will address comprehensively the nature and dimensions of this threat and the means to defeat it.

Third is the vulnerability of our cyber-enabled world to attack from outside as well as within. Computers and software are the linchpins of commerce, communications, care, education, defense…virtually all aspects of modern society. Worldwide, trillions of dollars are at risk. For example, the Supervisory Control and Data Acquisition (SCADA) systems used in petroleum refineries and other large industrial facilities are threatened by cyber-terrorists and criminal hackers lurking in the Internet. In 2000, Vitek Boden, fired from his job at an Australian sewage-treatment plant, remotely accessed the firm's computers and poured toxic sludge into parks and rivers, causing extensive damage. We must understand and defeat these and other cyber-threats to our safety and security.

While the realities of these threats and the operational requirements to defeat them focus our programs for safeguarding the nation's security, we are also mindful of the 9/11 Commission's finding that "the most important failure was one of imagination." We must never have a failure of initiative, agility or imagination again.

STRATEGIC GOALS AND OBJECTIVES

Our tasks and our duty are clear. We are mandated in law to develop and integrate strategies, policies, programs, operations, technologies and systems at every level of governmental operations that will enable the seamless protection of our way of life. This fundamental need goes to the very heart of The Constitution's obligation for the U.S. Government to provide for the common defense and the general welfare of the people.

To these ends, the Secretary of the Department of Homeland Security has articulated ***five strategic goals: (1) protect our nation from dangerous people; (2) protect our nation from dangerous goods; (3) protect critical infrastructure; (4) build a nimble, effective emergency-response system and a culture of preparedness; and (5) strengthen and unify DHS operations and management.***

S&T Strategic Framework

Critical objectives inform and shape DHS S&T plans, programs and activities:

:: Develop and deploy state-of-the-art, high-performance, affordable systems to prevent, detect and mitigate the consequences of Chemical, Biological and enhanced Explosive (CBE) attacks and disasters that require a federal response

:: Develop equipment, protocols and training for response to and recovery from CBE attacks and disasters

:: Enhance the technical capabilities of the Department's operational elements and other federal, state, local and tribal agencies to fulfill their homeland security-related roles, missions and tasks

:: Develop methods and capabilities to test and assess threats and vulnerabilities, anticipate emerging threats and prevent technological surprise

:: Develop technical standards and establish certified laboratories to evaluate homeland security and first-response technologies, and evaluate technologies for SAFETY Act protections

:: Support U.S. leadership in science and technology through basic research focused on filling phenomenology gaps that impede development of effective homeland security technologies and systems

Three elements of our homeland security posture are critically important to protect our nation, preserve our freedoms and support DHS strategic objectives. The most fundamental of these are the **highly skilled, committed and resolute people** who daily carry out millions of tasks, small and large, that contribute to national security. The second are the **strategies, doctrine, tactics, techniques and procedures** that shape how our people carry out their responsibilities. Third are the **technologies and systems** that our people use in their jobs every day to defend us against all threats and hazards.

The S&T Directorate functions as the nation's homeland security research, development, test and evaluation manager for science and technology. We manage an integrated program that focuses on Basic Research, Innovation and Transition to meet the needs of the DHS operating components and other federal government agencies; state, local

DHS S&T Customers and End-Users

Customers

- DHS operational components: Coast Guard, Customs and Border Protection, Domestic Nuclear Detection Office, Immigration and Customs Enforcement, Citizenship and Immigration Services, Federal Emergency Management Agency, Secret Service, Transportation Security Administration.
- DHS components that provide support to the operational components: Cyber Security, Emergency Communications, Health Affairs and Chief Medical Officer, Infrastructure Protection, Intelligence and Analysis, National Protection and Programs Directorate, Operations, Policy, Preparedness Directorate, Screening Coordination Office and US-VISIT
- Other federal law-enforcement departments, agencies and operational components.

End-Users

- More than 60,000 state, local and tribal public-safety agencies and jurisdictions in the United States, with their nearly 2.5 million emergency-response people.
- Owners and operators of the nation's critical infrastructure, spanning federal, state, local and tribal government organizations, including the private sector.

"As a Nation, we will emphasize science and technology applications that address catastrophic threats. We will build on existing science and technology whenever possible. We will embrace science and technology initiatives that can support the whole range of homeland security actors. We will explore both evolutionary improvements to current capabilities and development of revolutionary new capabilities".

National Strategy for Homeland Security — 2002

and tribal governments; and first responders and private-sector entities. Our Research, Development, Test & Evaluation program achieves compelling S&T strategic goals in **six fundamental disciplines: (1) Explosives; (2) Chemical and Biological; (3) Command, Control and Interoperability; (4) Borders and Maritime Security; (5) Human Factors; and (6) Infrastructure and Geophysical.** These are, as well, our six S&T Divisions.

In time-critical areas, the S&T Directorate delivers available technologies and systems to the people who need them, today. Focused, sustained long-term research is critical to make sense out of uncertainty and risk and to guarantee we will have the right tools for the complex problems we face.

To ensure that our efforts meet real-world requirements and deliver effective and affordable technologies, we established a customer-focused and output-based risk-analysis and requirements-assessment architecture that will provide revolutionary and game-changing capabilities. Our strategy-to-task framework directly links our programs and initiatives to specific strategic goals and customer requirements. Finally, the Directorate's management and oversight process tracks success in Product Transition in terms of **three objective metrics: project cost, schedule and technological readiness.**

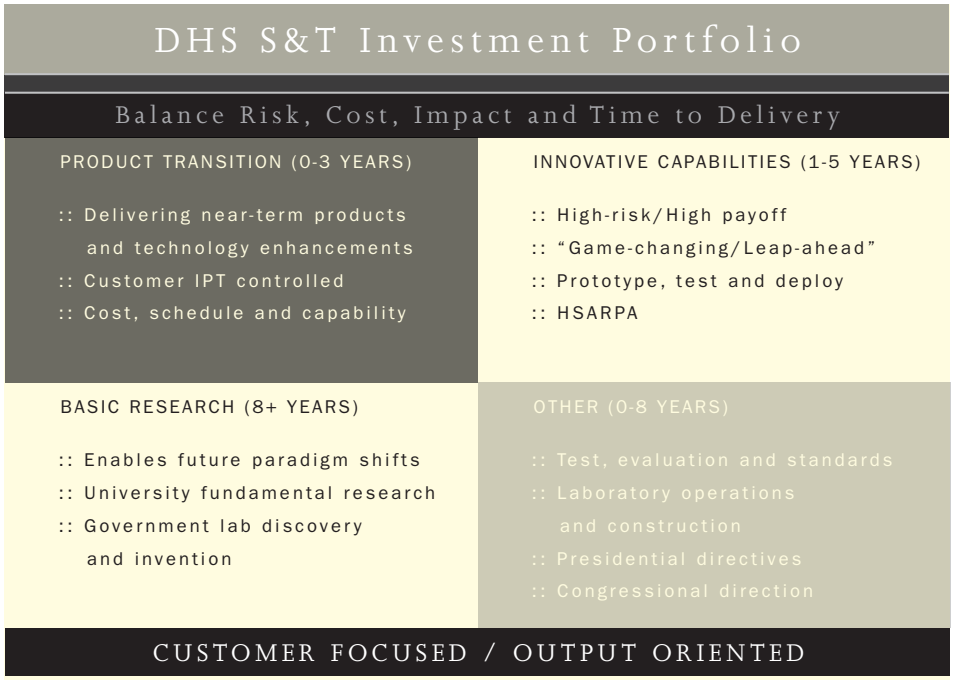
THE WAY FORWARD

The United States is at war with terrorism. The "front lines" can be overseas or they could be in the streets, ballparks, malls and subways of America's cities and towns…in our farms and our reservoirs…virtually anywhere a determined terrorist can deliver a weapon. The nation is also at risk from a broad spectrum of natural disasters, like the fires that devastated southern California in 2007 or the hurricanes that pelted the Gulf Coast in 2005.

We will never forget the horror of September 11, 2001 or the massive damage and human suffering spawned by natural disasters in recent years. The American people deserve a security posture that anticipates, detects, deters and responds to all threats and challenges. With a sharp focus on customers' needs and priorities—and with objective and measurable technical, schedule and cost metrics—we are pursuing advanced technologies to deliver results and gain the trust of the people. We are weaving the nation's safety net.

TWO :: FRAMEWORK FOR S&T SUCCESS

The S&T Directorate carries out an integrated investment portfolio comprising a broad array of many hundreds of programs and projects that balance risk, cost, mission impact and the time to deliver. Our portfolio includes long-term basic research, near-term product applications and leap-ahead, game-changing capabilities to satisfy critical operational needs. We know, too, that often the best solution-sets may cross the seams of the Homeland Security S&T Enterprise—comprising the S&T Directorate and our laboratories, other national laboratories, academia, and industry R&D organizations in the United States and overseas. Accordingly, we sustain and expand numerous cross-connections among S&T portfolios and divisions, DHS customers and first responders, and experts throughout the S&T Enterprise. We do not "do" S&T, but we do facilitate and invest in S&T—on occasion putting millions of RDT&E dollars at risk to reduce the risk of billions in acquisition and operations.

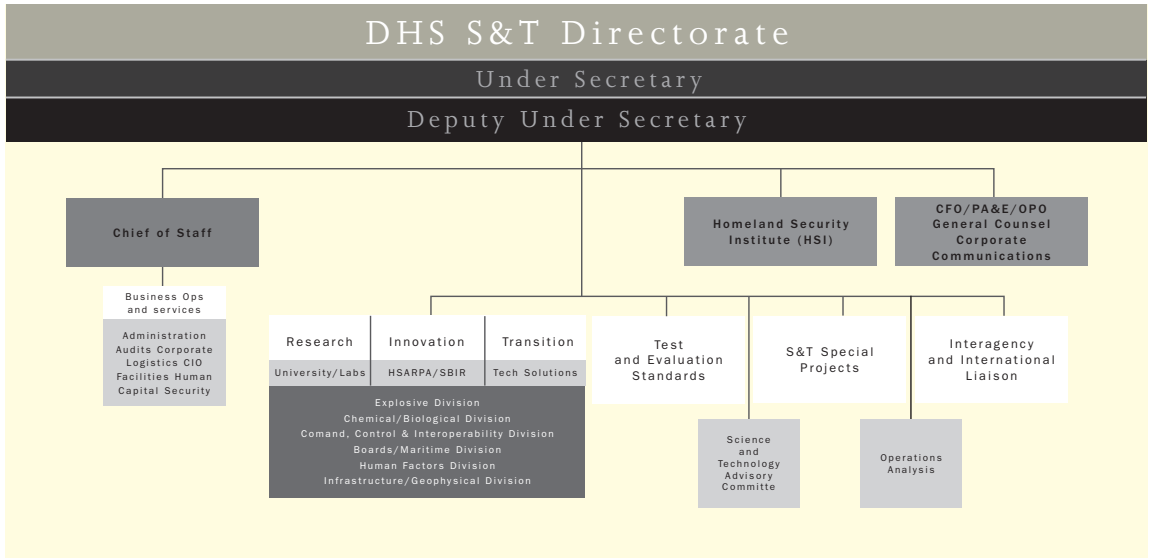


PUSHING S&T ENVELOPES

We carry out critically important programs and projects in three portfolio areas—**Basic Research, Innovation/Homeland Security Advanced Research Projects Agency and Product Transition**—and the six divisions listed on the previous page that collaborate closely to deliver innovative, substantial and relevant science and technology for our DHS customers and first responders. We pursue every program and project as a core element of our integrated investment portfolios, with key metrics—**cost, schedule and technological readiness**—for each.

Some 20 percent of the S&T Directorate's investment portfolio is in long-term Basic Research areas of enduring homeland security relevance, conducted primarily in universities and laboratories.

We cannot be risk-averse if we are to carry out our mission successfully. For that reason, we allocate about 10 percent of S&T funding to higher-risk, prototypical Innovation/HSARPA demonstrations that push the S&T envelope and which, if successful, will provide potentially game-changing technologies and systems in one to five years—much more quickly and with greater impact than the incremental improvements typical of most programs. And, we allocate about a tenth of the Innovation Portfolio—one percent of our total budget—to truly high-risk efforts, most of which, frankly, are likely to fail. Those that do bear fruit will have profound impacts on our security posture, while even the projects that "fail" will often result in enhanced understanding that helps focus subsequent basic and applied research and leads to breakthroughs and leap-ahead capabilities.



Another 50 percent of the S&T Directorate's investment is allocated to transition of lower-risk projects dedicated to satisfying DHS customer-defined capability needs, with spiral development, within three years. The remainder of our annual S&T program includes specially mandated programs and projects.

The S&T Directorate's Basic Research Portfolio addresses long-term research needs and oversees core DHS basic research programs and projects carried out by the six S&T divisions as well as collaborative programs with Homeland Security laboratories and other national labs, governmental agencies, universities and industry research programs. Basic Research supports fundamental S&T that could lead to paradigm shifts in America's homeland security capabilities, delivering revolutionary changes in the ways we meet enduring security challenges. Because of the long timeframe of these efforts—most looking eight years out and beyond—sustained, long-term, stable and focused research funded at sufficient levels is absolutely necessary to ensure a continuity of effort within the Homeland Security S&T Enterprise.

The Directorate's Innovation/HSARPA Portfolio focuses on two high-risk areas: (1) **High-Impact Technology Solutions** (HITS) projects that will provide proof-of-concept solutions within three years that could result in high-payoff technology breakthroughs; and (2) **Homeland Innovative Prototypical Solutions** (HIPS) projects that will deliver prototype-level demonstrations of game-changing technologies within five years. While these projects can be very risky, they offer prospects for truly dramatic and far-reaching improvements in capabilities.

In the James Bond thrillers, "Q" is the technological wizard who takes advantage of "boffins" throughout the British R&D community to ensure that "Agent 007" has the right stuff to save the world from some diabolical plot. So it is with the "HomeWorks" Office within Innovation/HSARPA. Similar to the famed aircraft "Skunk Works®" under Kelly Johnson during World War II and the Cold War, HomeWorks has a high degree of autonomy to manage HITS projects, in part because of their considerable risk of failure. This work represents an intermediate stage of the R&D process and is instrumental in revealing viable high-payoff R&D to pursue. The HomeWorks director also reaches out to non-traditional sources of homeland security insight and imagination.

Stranger than Fiction?

In addition to border agents, airport police and screeners, air marshals and maritime safety teams, we need people who can think well outside the "box"—unconstrained by the demands of daily operations. So, who better to help DHS balance more traditional thinking about homeland security than science-fiction writers? After all, Sci-Fi wordsmiths long ago told us about tourist spaceships and wireless handheld communicators—remember Dick Tracy's "Two-Way Wrist Radio" introduced into the comic strip in January 1946? And, while only a very few tourists can afford the trip into near-Earth orbit, cell-phones with video are now a way of life.

"Sigma" is a group of science-fiction writers that advises government officials on a broad spectrum of concerns, for example, what a post-nuclear attack age might look like. In 2007, S&T HomeWorks tapped Sigma to help consider the societal impacts of the revolutionary technologies being developed through Innovation/HSARPA programs, to think through how to deter and respond to terrorist attacks, and to plan for what follows should the unthinkable—a "dirty" WME detonated on Wall Street, for instance—occur. Other such thorny problems are also being addressed.

Sigma's ideas have groundings in reality: members of the group hold advanced degrees—most have PhDs—and others are medical doctors or professional engineers. The writers offer powerful imaginations that are supported by technical knowledge and can conjure diabolical ways in which our adversaries might strike. But they also develop ideas about how governments, communities and individuals might respond and what kinds of high-tech tools and tactics could prevent or mitigate attacks.

America gets much more than we "pay" for, as Sigma's members provide their services at no charge to DHS: "Science Fiction in the National Interest" is their motto. And for this group, nothing is unthinkable.

Courtesy of USA Today

REQUIREMENTS TO REALITY

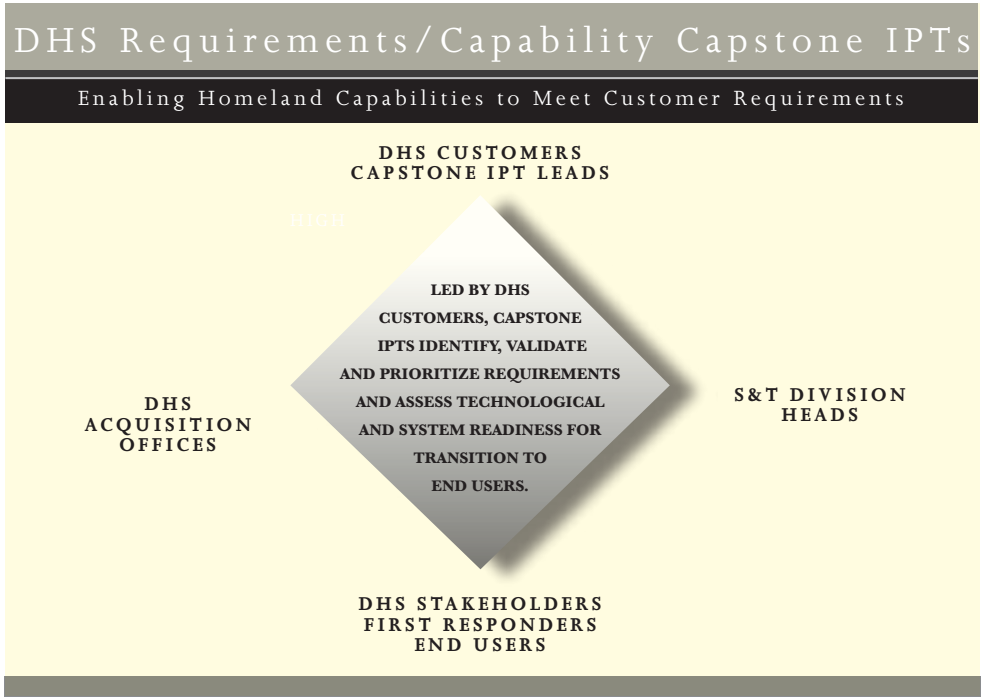
Research without results is of limited value, therefore the transition of advanced technologies and systems to the field is crucial for our security. We are committed to understanding our DHS customers' requirements and delivering, on time and within budget, capabilities that meet their strategic, operational and tactical needs. The American public deserves nothing less.

The Transition Portfolio is thus key to our integrated approach that: (1) assesses, prioritizes and funds requirements and programs on an annual basis; (2) responds to emergent or unanticipated needs; and (3) fields advanced technologies and capabilities as quickly as possible. We ask our customers' leaders, "What's keeping you awake at night?" And we pay very close attention to their answers.

The DHS customer-led Capstone Integrated Product Teams (IPTs) are critical nodes in the process to determine operational requirements, assess current capabilities to meet operational needs, analyze gaps in capabilities and articulate programs and projects to fill in the gaps and expand competencies. The Capstone IPTs actively engage DHS customers, acquisition partners, S&T division heads and end-users in our RDT&E and acquisition activities. IPTs can also include other federal partners outside DHS who offer or require advanced technologies. Each IPT identifies, validates and prioritizes requirements for the S&T Directorate and provides critical input to investments in programs and projects that will ultimately deliver technology solutions that can be developed, matured and delivered to our customers' acquisition programs for deployment to the field. Twelve Capstone IPTs are active in 2008:

:: Border security
:: Maritime security
:: Cargo security
:: Chemical and biological defense
:: Cyber-security
:: Transportation security
:: Incident management
:: Information sharing and management
:: Infrastructure protection
:: Interoperability
:: People screening
:: Counter-IED

We also know that a successful Transition Portfolio requires sustained customer feedback from DHS components to ensure that our programs address genuine capability gaps. To gain this insight, we have established 46 Project IPTs and semi-annually reach out to DHS components to gauge their overall satisfaction with delivered products and capabilities as well as ongoing Transition Office activities. The results are explicitly tied to outcome-based performance metrics of cost, schedule and technology readiness. We know when we do well and recognize if improvement is needed.



Protecting You, Protecting U.S.

Ingenuity and invention are the lifeblood of robust research and development, and nowhere is that better seen than in America's high-tech arenas. Large as well as small firms can be high-powered "engines" of counter-terrorism imagination and leading-edge solutions. But potential legal liabilities could stifle the entrepreneurial spirit for developing disruptive and enabling technologies and products.

The* Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act *of 2002 is a valuable tool for expanding the creation, proliferation and use of cutting-edge anti-terrorism technologies and products. Qualified anti-terrorism technologies include products, software, hardware and services that help deter, prevent, detect, identify or respond to acts of terrorism and limit the harm such acts might cause. The S&T Directorate administers three levels of liability protection for sellers and users of anti-terrorism technologies:

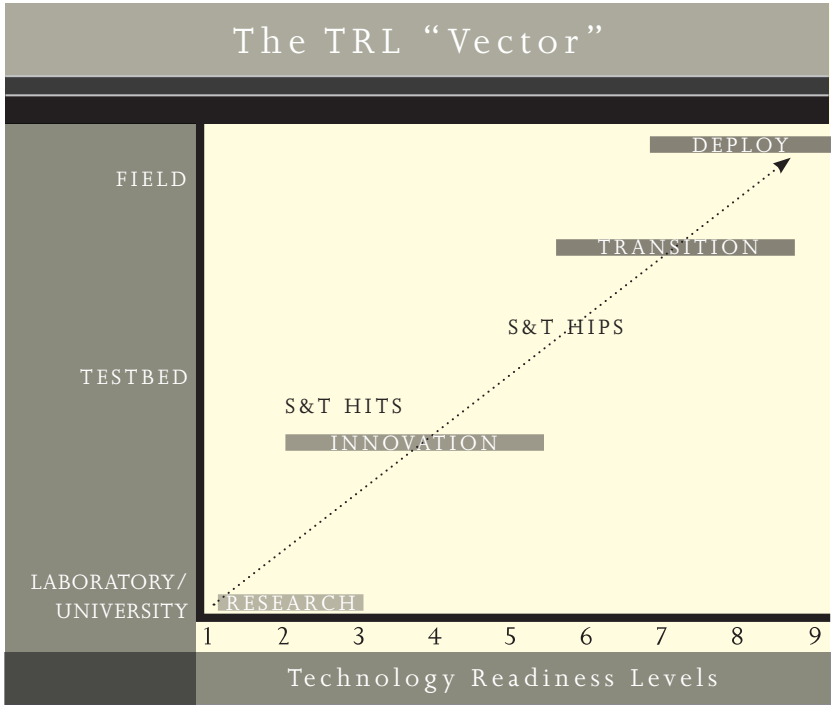
- **Developmental Testing & Evaluation Designation:** ***Liability protection for products or services that have demonstrated potential effectiveness during testing and evaluation. Liability is capped at the level of liability insurance that DHS determines to be appropriate for an agreed testing plan, which can include limited operational deployments. Coverage remains in force for up to three years.***
- **Designation:** ***Liability protection for products or services that have demonstrated effectiveness, such as successful performance in an operational environment. The insurance requirement is set by DHS and is based on various factors, including the nature of the technology, risks related to its intended deployment and the cost and availability of the insurance. Designation will last for five to eight years.***
- **Certification:** ***Liability protection for certified products or services that meet the criteria for Designation and for which there is a high confidence they will perform as intended and be effective. These technologies are placed on the DHS Approved Products List. Certification provides significantly enhanced protection by allowing the seller to assert the Government Contractor Defense for claims arising from acts of terrorism. Certification will last for five to eight years.***

A total of 179 approvals have been awarded through FY 2007. Last year, alone, 81 new technologies and services were approved for SAFETY Act coverage—an 83 percent increase compared to the previous three years of the program. Nearly 90 percent of the 2007 awards have direct relevance for capabilities and needs identified by the Capstone IPTs.

MEASURING OUR SUCCESS

"Success" means making America safer. We carefully manage the taxpayers' dollars entrusted to us to achieve that fundamental goal. We do this by satisfying our DHS customers' and America's first responders' needs, on time and within established budgets. To help ensure success, we establish explicit **cost, schedule and technological readiness metrics for each project.**

Cost is always important, and we must provide the S&T foundations for affordable, maintainable and effective technologies and systems. We know that we must accurately estimate and track the RDT&E cost of a technology or system so intelligent and informed decisions can be made at critical junctures in its development and testing. We will "weed out" under-performing projects to free up scarce resources for more promising initiatives. Finally, we are mindful that, once in the field, technologies and systems must be operated effectively and easily maintained; an advanced system that cannot be used because of false alarms, inadequate training or lack of spare parts is of little value.



We also establish detailed timelines, plans-of-action and milestones to monitor each project's progress. Frequent program reviews and internal assessments allow us to identify and correct early on any problem that might frustrate our ability to deliver the technology or system to our customers when they need it. Our Transition Office also formally elicits customer feedback from DHS components within the Capstone IPT process to ensure individual projects remain on track.

Finally, we are using the well-established Technology Readiness Levels (TRLs) for a systematic measurement system to support periodic assessments of the maturity of a specific technology or system. The TRLs also support determining whether a capability solution is ready to be transitioned to the field or should be restructured or discarded.

A GLOBAL PERSPECTIVE

Good ideas that enhance U.S. homeland security know no boundaries—either bureaucratic or international. In no small measure, our success in navigating the basic research-to-deployment continuum depends on technical and scientific support from numerous governmental, academic and commercial organizations. An increasingly important DHS S&T outreach activity maintains contacts with scientists, engineers and managers throughout the world to help meet critical needs and to support innovative S&T approaches. Safeguarding America's security is an "all-hands" effort that also requires close collaboration with allies, friends and partners worldwide.

THREE :: AN "ALL HANDS" EVOLUTION

"Not Invented Here!" has been embraced enthusiastically within the S&T Directorate, but not at all in the usual connotation of the phrase.To be successful, we look well beyond our department and even America's borders for imaginative and cost-effective "NIH" solutions to combat terrorism and enhance response to natural disasters. We are drawing upon RDT&E capabilities across the Homeland Security S&T Enterprise in the United States as well as overseas to achieve optimum solutions that balance cost, capabilities and time-to-delivery. We are pushing the discovery and invention envelope at home and throughout the world to develop and acquire advanced technologies and systems that undergird security.

Focused S&T Communications

Nothing is more important than the ability to communicate effectively. To ensure the right information gets to the right people at the right time, to guarantee that we will never have "a failure to communicate," we have established a dedicated corporate communications office charged with supporting all S&T Directorate elements. The goal of our communications team is to educate, inform and encourage the participation of federal, state, local, tribal, private sector, academic and other domestic and international organizations. Under DHS leadership, S&T "Comms" prepares and carries out public and legislative affairs strategies, plans, programs and initiatives, including structured congressional and public media events; three annual stakeholder conferences held in Washington, DC, on the West Coast and overseas; a robust global exhibit program; and special-focus seminars and materials. Other S&T points of contact are:

:: Basic Research: S&T-Research@dhs.gov

:: Innovation/HSARPA: S&T-Innovation@dhs.gov

:: Transition: S&T-Transition@dhs.gov

:: Explosives: S&T-Explosives@dhs.gov

:: Chemical & Biological: S&T-ChemBio@dhs.gov

:: Command, Control & Interoperability: S&T-C2I@dhs.gov

:: Borders & Maritime: S&T-BordersMaritime@dhs.gov

:: Human Factors: S&T-HumanFactors@dhs.gov

:: Infrastructure Protection & Geophysical Science: S&T-InfrastructureGeophysical@dhs.gov

:: SAFETY Act: Helpdesk@safetyact.gov

:: TechSolutions: Techsolutions@dhs.gov

:: Interagency Programs: Interagency.Programs@dhs.gov

:: International Programs: International.Programs@dhs.gov

:: Operational Analysis: OA.Programs@dhs.gov

:: Homeland Security Institute: www.homelandsecurity.org

:: Special Programs: Special.Programs@dhs.gov

:: Test & Evaluation: T-and-E.Programs@dhs.gov

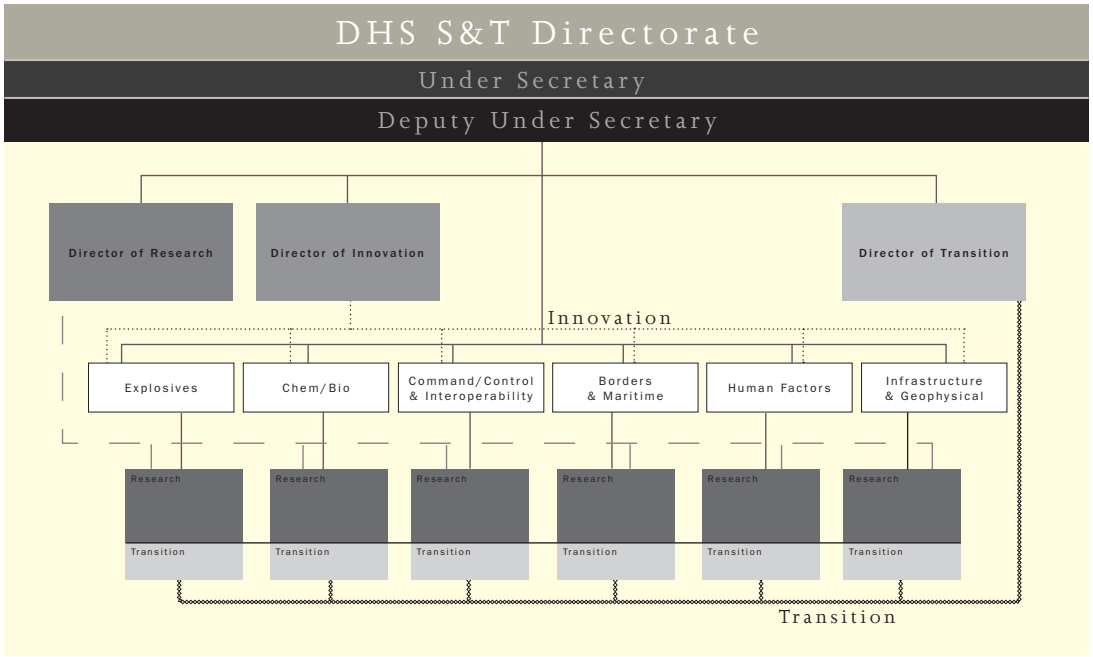
:: Standards: Standards.Programs@dhs.gov

:: Office of National Labs: ONL.Programs@dhs.gov

:: University Programs: www.dhs.gov/universityprograms

:: Corporate Communications: Corporate.Communications@dhs.gov

We actively pursue numerous domestic and international outreach initiatives that support our mission and our customers. In addition to the DHS laboratories and research centers, for example, the S&T Directorate uses other government agencies' research resources, including those of the Departments of Agriculture, Defense, Energy, Justice and Health and Human Services; the Environmental Protection Agency, the National Institute of Standards and Technology and the National Science Foundation; and the Department of Defense (DoD) Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs). Additionally, we reach out to industry and stakeholder associations for their insight and expertise. We are also nurturing, expanding and sustaining a government-academia-industry team that will allow us to meet the dynamic and daunting S&T challenges for a more secure America. S&T Interagency and International Program Offices coordinate with other Executive Branch agencies and reach out to international partners to tap into science and technology communities worldwide for effective and affordable solutions to our security needs. And we have put in place an innovative means to get recommendations from first responders in the field—our ultimate customers—at **TechSolutions@dhs.gov.** The key to our success in these critical activities is our people.



THE HUMAN "ELEMENT"

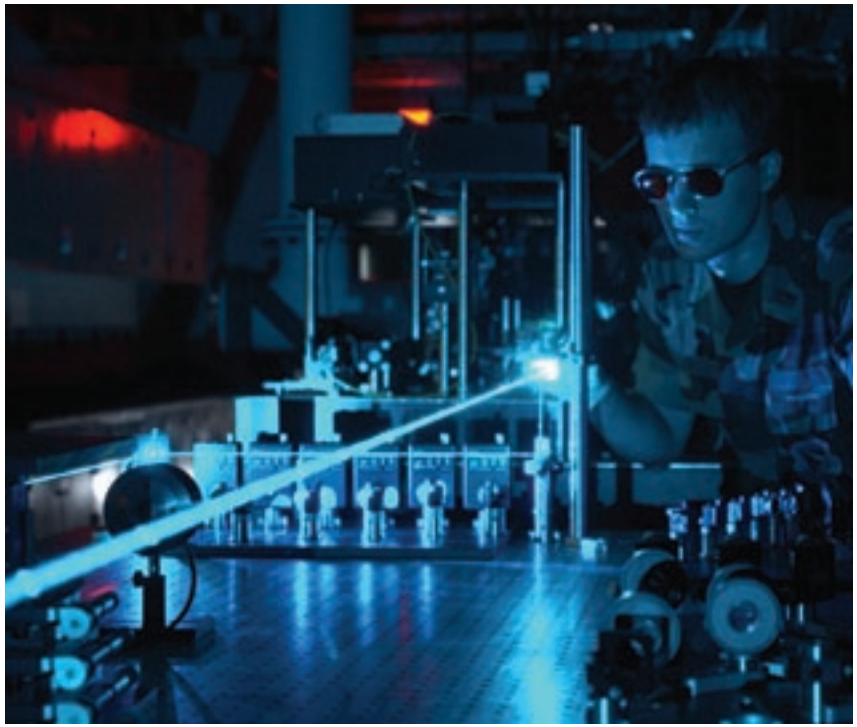
Our most valuable asset is not cutting-edge technology or new equipment, but rather our highly skilled, dedicated, flexible and agile team of S&T professionals. Without any doubt, our success depends on our people and their leadership of the Homeland Security S&T Enterprise—the transformation engine for America's security. We have shaped a work environment in which our people are encouraged and rewarded for using initiative to anticipate and improvise to changing circumstances or sudden opportunities.

TECHSOLUTIONS

No one understands the needs of first responders better than first responders. Every day, hundreds of law-enforcement officers, firefighters, emergency medical services personnel and bomb-squad members think: "There's gotta be a better way to do this!" In many cases, they are right.

The S&T Directorate's Technology Clearinghouse and TechSolutions initiatives are the means for first responders to contact the Directorate, let us know what they need and get direct support to help them do their jobs more rapidly, effectively and safely. Established by the 2002 Homeland Security Act to provide "one-stop shopping" for advanced technology information to support federal, state and local public-safety and emergency-responder communities, the S&T Technology Clearinghouse provides information on products and services to assist first responders in making informed procurement decisions based on performance tests and evaluations, to accelerate the development of technical and operational standards and to provide best-practice forums to share information on training, tactics, techniques and procedures.

TechSolutions is a web-based method for first responders to submit directly to DHS S&T their concerns about high-priority capability gaps and generate opportunities for rapid prototyping to help them in their jobs through **www.firstresponder.gov**. TechSolutions informs DHS, other federal agencies and the private sector of the emergency-responder community's needs; identifies existing technology that could meet the needs; or, if no technologies or systems are available, S&T proceeds with the rapid prototyping of solutions to be fielded in less than 12 months and at a total cost of no more than $1 million. Proposals can be under way in less than 45 days. TechSolutions and the Technology Clearinghouse help speed the deployment of critical technologies, systems and capabilities to where they are needed most.



SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE

The Homeland Security Act of 2002 directed the establishment of a Homeland Security Science and Technology Advisory Committee to be a source of independent scientific and technical planning advice for the Under Secretary. The Committee comprises 20 members, eminent in fields such as emergency response, research, engineering, new product development, business and management consulting. They are appointed on the basis of established records of distinguished service and are selected to provide a cross-section of the RDT&E and implementation expertise; none are federal employees. The Committee assists the Under Secretary in establishing mission goals for future S&T; identifies research areas of potential importance to national security; advises on whether the policies, actions, management processes and organization constructs of the S&T Directorate are focused on mission objectives; advises on whether the Directorate's RDT&E and systems engineering activities are properly resourced; identifies outreach activities; and reviews the technical quality and relevance of the Directorate's programs.

INTERAGENCY OUTREACH

The Interagency Programs Division coordinates with other U.S. Executive Branch agencies to identify unmet needs, avoid duplication and collaborate with science and technology communities throughout the government for solutions. For example, there are numerous intersections of homeland security, homeland defense and national security missions, and the Directorate is teaming with the Defense Department and industry to address seams, overlaps and gaps in meeting civilian security and military defense S&T needs. A particular focus in 2008 is to expand the S&T Directorate's liaison with the U.S. Northern Command (NORTHCOM) at Peterson Air Force Base, Colorado, and the U.S. Joint Forces Command (JFCOM), headquartered at Norfolk, Virginia, for advanced concept experimentation and exercises.

S&T's Interagency Programs also develops, in consultation with other executive agencies, the government's national policy and strategic plan to identify, establish and communicate priorities, goals, objectives and policies regarding countermeasures to chemical, biological and other emerging terrorist threats. This effort involves articulating comprehensive, research-based definable goals and measurable objectives to accomplish and evaluate interagency efforts. In addition, along with TechSolutions and the Office of Interoperability and Compatibility, the Interagency Office provides for a general first-responder interface directly with S&T Directorate.

INTERNATIONAL COLLABORATION

The world is indeed flat! Just as we are reaching out to the American S&T community-at-large, we are also looking beyond the United States for innovative and effective solutions in combating terrorist threats and responding to natural disasters that respect no borders or frontiers. The International Programs Division has crafted a strategic program of proactive and focused international cooperative S&T programs and projects with governments, industry and academia worldwide. Our initiatives have catalyzed global connectivity among the international S&T community, the Homeland Security S&T Enterprise, DHS operational components and the Department of State to address common interests and high-priority requirements.

For example, in addition to programs focused on the Western Hemisphere, three senior liaisons address international S&T partnerships in Europe, Russia/Eurasia and the Pacific Rim/Asia, while an international S&T grant program augments and complements—through international research and collaboration—the Directorate's efforts. Several government-to-government Memoranda of Agreement (MoAs) provide an umbrella framework for cooperation to conduct international RDT&E, share data, leverage resources and eliminate unnecessary duplication for high-priority technologies and systems. Bilateral MoAs are in place with Australia, Canada, Singapore, Sweden and the United Kingdom, and during 2008 we will seek to partner with Israel, Germany, the European Union, Mexico and New Zealand. Under our MoA with Sweden, for example, in 2007 we conducted a bilateral exercise to identify S&T requirements to mitigate the effects of IEDs in mass-transit systems, and a 2008 exercise will address joint approaches for Maritime Domain Awareness and enhanced port and waterway security.

Our collaboration often is at the tactical level and in real time. During the liquid-explosives airline security incidents in 2006, for example, when 24 terrorists were arrested after plans to smuggle seemingly innocuous liquids and detonating devices on several transatlantic aircraft were uncovered, U.S. and British explosives experts shared S&T data and law-enforcement information. Subsequent tests showed just how deadly even a small amount of explosives made from readily available ingredients could be. Similarly, in the immediate aftermath of the 2007 attempted London and Glasgow bombings, close U.K./U.S. collaboration helped unravel the plots and arrest alleged perpetrators.

Annual S&T conferences with our key international partners also help set the global agenda for homeland security RDT&E, manage scientist and engineer exchange programs with several countries, and develop joint strategic R&D programs with each DHS S&T division that link to partner nations on mutually beneficial research projects or to respond to a crisis. An "S&T Stakeholders and Partners" conference was held in London in 2007, and future conferences are being planned for the Asia-Pacific region and Sweden.

The United States is not alone in this fight, and international outreach and teaming are vitally important to America and our worldwide partners. As Benjamin Franklin warned more than 230 years ago: "Either we all hang together, or most assuredly we shall all hang separately." It is a caveat that all nations must heed if homeland security worldwide is to be enjoyed.

ANALYSIS AND EXPERIMENTATION

The Director of the Operations Analysis (OA) Division is the Under Secretary's primary advisor on requirements for operations analysis, war gaming and experimentation. Specific responsibilities include:

:: Initiating and conducting operations analysis projects within the S&T Directorate

:: Providing operations analysis, including risk-informed decision analysis, and war-gaming support to the Capstone IPTs that establish department-wide priorities for S&T programs and projects to be pursued within budgetary constraints

:: Supporting assessment of S&T proposals to help determine which are critically important to the S&T program and should be funded by DHS S&T

:: Serving as Executive Agent of the Homeland Security Institute, the nation's first Federally Funded Research and Development Center concentrating exclusively on homeland security

:: Overseeing and managing the Department's use of other FFRDCs

Homeland Security Institute

A key instrument in the S&T Directorate's "toolbox," the Homeland Security Institute is a specialized studies and analysis FFRDC established by the Homeland Security Act of 2002. The Institute provides a unique source of in-depth knowledge of homeland security mission objectives, operational concepts and requirements, strategies, resources, systems and technologies. The Institute's mission is to assist the Department of Homeland Security and its operating elements in addressing important homeland security issues, particularly those requiring scientific, technical and analytical expertise. The research agenda covers the spectrum of homeland security issues and activities, including threat trends and adversarial perspectives, information sharing and communications interoperability, border and transportation security, law enforcement, infrastructure protection, preparedness, emergency response and training.

Experimentation is critical to success, and the OA Division promotes experimentation to evaluate and validate competing concepts of operations, new systems concepts and ongoing projects. The division's experimentation and war-gaming capabilities are also shared throughout the DHS and are important for effective liaison with other federal agencies and overseas organizations. Maturing programs with the Defense Department's Northern Command, Joint Forces Command and other Combatant Commands, for example, are investigating "joint" concept development and experimentation for integrated and coordinated DHS/DoD civil-military responses to national emergencies. These include the collaborative development and testing of high-altitude, persistent unmanned aerial vehicles and mission packages for robust command, control and communications in national defense and domestic disaster-relief operations. Another vital requirement is for civilian and defense collaboration in ports and waterways security, which includes anti-terrorism and force-protection of the Navy's ships in U.S. homeports, as well as overseas. Here, the OA Division is helping to shape and carry out experiments to test assumptions and evaluate programs aimed at a variety of water-borne threats to military, commercial and private vessels and the maritime transportation system.

SPECIAL PROGRAMS

Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy, but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.

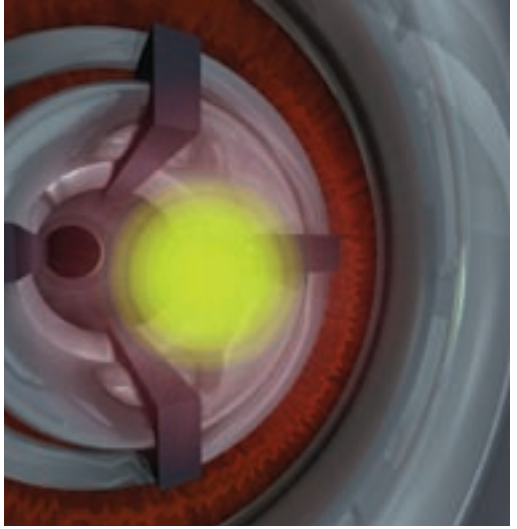
Sun Tzu
The Art of War

The Special Programs (SP) Division coordinates classified R&D projects and focuses on emerging threats, risk sciences, aircraft and Unmanned Aerial Vehicle (UAV) detection and development, as well as other homeland-security areas that may be especially sensitive, classified or deserving of extraordinary security protection. Special Programs is the S&T conduit for coordination among DHS and other U.S. and foreign government and international agencies for initiatives and programs involving sensitive technologies, especially those that might not align well with S&T's six technical divisions. SP also provides a vital liaison between DHS S&T and the Department of Defense and the Intelligence Community for common concerns.

The SP Emerging Threats Branch addresses the dynamic nature of technological advancements and fosters long-term, creative exploratory RDT&E programs to anticipate and counter new and dynamic threats. We use innovative, crosscutting approaches to determine potential threats resulting from advances in technology or terrorist use of existing capabilities in new or unexpected ways. Our goal is to derive potential counters in less than 18 months and deliver quick-fix solutions or initiate traditional acquisition programs.

The SP Risk Sciences Branch provides sound approaches for the creation and use of risk information in decision-making across the Homeland Security S&T Enterprise. The branch also conducts a comparative studies program that focuses on terrorism and other homeland-security threats as competitions between intelligent, adaptive, reactive and strategically driven adversaries. From this chess-like perspective, we analyze interactions between two or more sides that will shape competition over time, rather than a single move. Our adversary's possible and probable actions and reactions are explicitly addressed as we determine specific security measures.

Finally, SP's Aircraft/Unmanned Aerial Vehicle Detection and Development Branch—in coordination with the Directorate's Command, Control and Interoperability and Borders/Maritime divisions—merges unmanned airborne platform development with the DHS airspace requirements to detect correlated and un-correlated tracks within the National Airspace System. The branch provides the expertise necessary for strong partnership with DHS' aviation-support providers. This partnership enhances the Department's ability to employ airborne platforms to detect, track, interdict and apprehend conveyances and people conducting illegal activities. The branch also provides a unified perspective on aviation support for homeland-security decision-making.



T&E/Standards Key Achievements

:: Chemical, Biological, Radiological, Nuclear and Enhanced Explosives (CBRNE) sensors and detection equipment standards

:: X-ray and gamma-ray technical performance standards, including detection standards for bulk explosives, weapons and contraband

:: Interagency standards for decontamination technologies, protocols and training

:: Standards supporting first responders: Incident management standards, communications standards, CBRN protective equipment and urban search-and-rescue robots standards

:: Standards for Biometrics: Latent fingerprint analysis standards, rapid biometric evaluation standards and biometric image and physical feature quality standards for identity cards and travel documents

:: Standards for biometric image and physical feature quality for identity cards, such as the Transportation Worker Identification Credential (TWIC)

:: Test & Evaluation policies and processes

Test & Evaluation/Standards

Technical standards are essential for effective, coordinated response to incidents that span numerous jurisdictions and diverse emergency-responder disciplines and needs. They are crucial for crafting and then testing and evaluating homeland security technology solutions that are integral to systems comprising multiple components and must link together seamlessly in a "plug-and-respond" environment.

The S&T Directorate's Test & Evaluation and Standards Division has integrated T&E and Standards into the DHS development and acquisition cycle through continuous evaluation of system test requirements, planning and execution. We have established four standards working groups—CBRNE Countermeasures Standards; Emergency Preparedness and Response Standards; Border and Transportation Safety Standards; and Standards Process and Infrastructure Development—to ensure that equipment and tools are safe, reliable and affordable and our customers' needs are met.

The program also establishes policy and procedures for DHS test and evaluation and provides independent T&E and assessment. In these efforts, the program works across DHS components to coordinate T&E resources, ensure capable T&E infrastructure is in place, and verify technical performance, operational effectiveness and suitability for transition and deployment.

OFFICE OF NATIONAL LABS

The S&T Directorate's Office of National Laboratories (ONL) develops, sustains and expands a coordinated network of DHS and Department of Energy National Laboratories and other federal labs and centers to help deliver critical homeland capabilities. In addition to its oversight and funding of DHS laboratory operations, ONL coordinates and aligns with the six S&T technical divisions the myriad homeland-security activities throughout the U.S. R&D community.

The ONL "Harvesting Innovation" project, for example, has already improved the way that the S&T Directorate can leverage the scientific and technical expertise at national facilities. "Harvesting Innovation" gathers detailed information about efforts supporting Laboratory-Directed Research and Development (LDRD) programs and shares this with DHS directors, division heads and program managers. Energy Department labs allocate some $400 million per year in LDRD, approximately $90 million of which is related to homeland-security requirements. To facilitate information exchange, ONL uses specialized software to correlate LDRD projects with DHS S&T strategic goals and ongoing programs as well as planned projects in all six S&T divisions. This minimizes duplication of effort and maximizes the nation's return on its homeland-security S&T investments.

Co-located with the Department of Defense Edgewood Chemical and Biological Center in Maryland, the Directorate's S&T **Chemical Security Analysis Center** (CSAC) provides the scientific foundation for the awareness of chemical threats and how they might be used against us. The CSAC maintains an extensive computer-based clearinghouse of chemical hazards data and carries out special projects in support of DHS and inter-agency requirements.

Since 1947, the **Environmental Measurements Laboratory** (EML) in New York City has focused on worker occupational health and safety as well as monitoring and radiation detection. Today, EML also carries out pilot-deployment projects in many more areas, including: helping the New York Police Department choose and maintain hand-held radiation-detection devices; training first responders on the impact and measurement of "dirty bomb" and other WME threats; devising systems to monitor ports, bridges and tunnels for signs of nuclear terrorism; testing a rail security system to detect leave-behind explosives and suicide bombers; and working on detecting materials in containers on board ships in transit. With the DHS Domestic Nuclear Detection Office (DNDO), EML promotes radiation-countermeasures technologies and standards, supports technical reach-back, and provides technical assistance on radiation monitoring and protection.

DHS S&T Lab Partners

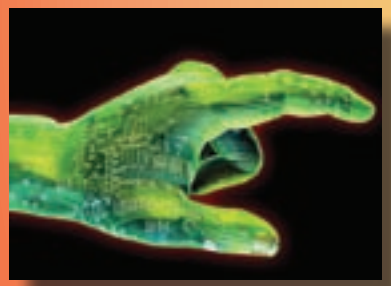
Department of Energy National Laboratories

- :: Argonne National Laboratory
- :: Brookhaven National Laboratory
- :: Idaho National Laboratory
- :: Lawrence Berkeley National Laboratory
- :: Lawrence Livermore National Laboratory
- :: Los Alamos National Laboratory
- :: Nevada Test Site/Remote Sensing Laboratory
- :: Oak Ridge National Laboratory
- :: Pacific Northwest National Laboratory
- :: Sandia National Laboratories
- :: Savannah River National Laboratory

S&T Directorate In-House Laboratories and Centers

- :: Chemical Security Analysis Center
- :: Environmental Measurements Laboratory
- :: National Biodefense Analysis and Countermeasures Center
- :: Plum Island Animal Disease Center
- :: Transportation Security Laboratory

12 Capstone IPTs Address Critical Needs



- Border Security >>
- Maritime Security >>
- Cargo Security >>
- Chem/Bio Defense >>
- Cyber Security >>
- Transportation Security >>
- Incident Management >>
- Information Sharing >>
- Infrastructure Protection >>
- Interoperability >>
- People Screening >>
- Counter-IED >>

179 Critical Projects Under Way in 2008

BORDERS & MARITIME: ACSD. ASAT. Boarding Officer Tools. Border Officer Tools. Border Detection Grid. Border Net. Composite Container. CSD. MATTS. SBI Systems Engineering/Modeling & Simulation. SCSA. Sensor Data Fusion & Decision Aids.

CHEMICAL & BIOLOGICAL: Autonomous Rapid Facility Chemical Agent Monitor. BioForensics R&D Near Term. BioForensics R&D Far Term. BioWatch Gen-3 Detection Systems. BioAssays Near Term. BioAssays Next Generation. BioDefense Knowledge Center. BioDefense Net Assessments. BioForensics Operations/ NBFAC. Biological Warning & Incident Characterization. BioThreat Characterization Center. BioWatch Gen-2 Operations. Next Generation BioWatch Procurement. Chemical Decontamination R&D. Chemical Forensics & Attribution. Chemical Security Analysis Center. Detect-to-Protect Remote Sensors. Detect-to-Protect Triggers & Confirmers. Facility Restoration Demonstration. FAD Modeling. FAD Vaccine & Diagnostics. Fixed Laboratory Response Capability. Food Biological Agent Detection Sensor. Integrated CBRN(E) Detection System. Joint AgroDefense Office. Lightweight Autonomous Chemical Identification System. Low Vapor Pressure Chemical Identification System. Low Vapor Pressure Chemical Detection System. NBIS. Next-Gen ARFCAM & LACIS. Operational Tools for Response & Restoration. Portable High-Throughput Integrated Laboratory Identification System. Rapidly Deployable Chemical Detection Systems. Systems Studies. Systems Approaches for Restoration.

COMMAND, CONTROL & INTEROPERABILITY: All-WME. Architecture & Framework. Compliance Assessment. Countermeasures Development and Detection. Cyber Security Assessment. Cyber Security Testbed-Experimental Research Testbed. DNSSEC-Secure Protocols. Cyber Security Experiments & Exercises. ICAHST. Identification & Assessment. IFSL Information Sharing. Interoperability Migration Project. Large-Scale Datasets-Research Data Repository. Next-Generation Technologies BAA 04-17 07-09. Outreach. Public Safety Architecture Framework. SPRI-Secure Protocols. Standards & Modeling-P25 Interfaces. Statements of Requirements. Interoperability Technology Demonstrations. Visual Analytics & Physics-Based Simulation.

EXPLOSIVES: Air Cargo. Aircraft Hardening. Algorithm & Analysis of Raw Images. Bomb Assessment Technologies & Integration. Counter-MANPADS Interagency Evaluation. Detection & Neutralization Tools. Detection Technology & Material Science. Fundamental Particle Physics. GUARDIAN System Evaluation. Home Made Explosives. Improvements to Deployed Checked Baggage Technology. JETEYE System Evaluation. Liquid and Home Made Explosives Chemical Characterization. Manhattan II. Next-Generation Carry-On Detection. Next-Generation Passenger Checkpoint. Special Programs Office.

HUMAN FACTORS: Biometrics. Community Perceptions of Technologies Panel. Credentialing-Personal Identification Sytems. Enhanced Screener-Technology Interface. Enhancing Public Response and Community Resilience. Group Violent Intent Modeling and Simulation. Risk Perception, Public Trust & Communication. Hostile Intent.

INFRASTRUCTURE & GEOPHYSICAL: Advanced Concepts & Special Studies. Blast/Projectile Protection. Community-Based CIP Institute. Dashboard Development. IMACC. CIP-DSS Interdependence Model Build-Out. National CIP R&D Plan. Personal Protection Equipment. Regional Technology Integration Initiatives-Anaheim, Cincinnati & Seattle. Sector & Threat-Specific MSA. Sector-Specific Risk Reduction. Southeast Regional Research Initiative. Training, Exercise & Lessons Learned. Unified Incident Command & Decision Support.

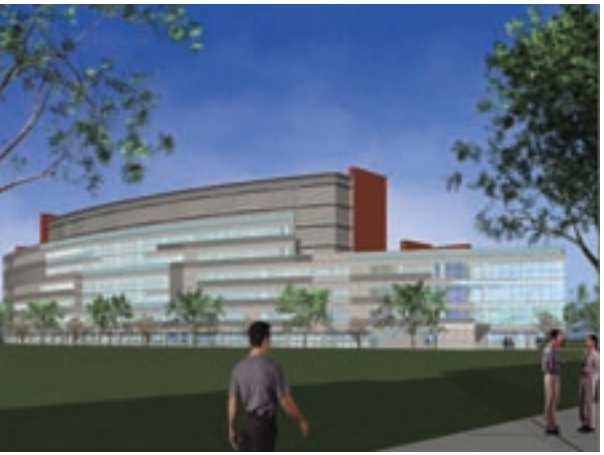
INNOVATION: Biometric Detector. Cell-All Ubiquitous Chem/Bio Detection. Critical Infrastructure Change Detection. Document Validator. First Net. Future Attribute Screening Technologies. Hurricane and Storm Mitigation. IED Defeat. Levee Strengthening and Damage Mitigation. CHLOE. Real-Time Bio Detection. Resilient Tunnel. Resilient Electric Grid. SAFECON. Scaleable Common Operating Picture Experiment. MagViz NMRI. Tunnel Detection.

LABORATORY FACILITIES: CSAC Operations. EML. NBACC Operations. NBAF Construction. Plum Island Disease Center Operations & Upgrades. PNNL 300. TSL Operations.

T&E/STANDARDS: ANSI. Biological Countermeasures Standards. Biometrics Equipment Standards. BioThreat Detection Hand-Held Assay Second-Round Testing. Cargo Security Technology Standards. Chem/Bio Threat Response & Recovery Validated Sampling Plans. Chemical Countermeasures Standards. Communication Standards. Countermeasures Testbed Closeout. Credentialing-Human Factors. Explosives Countermeasures Standards. GIS Interoperability Standards. IEEE. Incident Management Training & Process Standards. INCITS. Interoperable Communications T&E. NIMS Integration Center/EML. Personal Protective Equipment for Responders. RFID. Standards Infrastructure Development. T&E Development & Analysis. T&E Infrastructure Development. T&E Policy Analysis & Development. TWIC. Urban Search & Rescue Robots Standards. X-Ray Screening Equipment Standards.

TRANSITION: International & Interagency Programs. SAFETY Act. Technology Clearinghouse.

UNIVERSITY PROGRAMS: Center of Excellence (CoE) for Border Security & Immigration. CoE for Explosives Detection, Mitigation & Response. CoE for Maritime, Island & Port Security. CoE for Natural Disasters, Coastal Infrastructure & Emergency Management. CoE for Transportation Security. The Center for Risk and Economic Analysis of Terrorism Events (CREATE). The Center for Advancing Microbial Risk Assessment (CAMRA). The National Center for Foreign Animal and Zoonotic Disease Defense (FAZD). Discrete Sciences Centers. Joint DHS-CoE Competitions. Minority-Serving Institutions. The Center for Food Protection and Defense (NCFPD). The National Center for the Study of Preparedness and Catastrophic Event Response (PACER). Regional Visualization & Analytics Centers. Scholars and Fellows. The National Consortium for the Study of Terrorism and Responses to Terrorism (START).



The **National Biodefense Analysis and Countermeasures Center** (NBACC) is the first DHS lab to be designed and constructed specifically to address critical threats, requirements and technologies. Located at the U.S. Army's National Interagency Biodefense Campus at Fort Detrick, Maryland, the NBACC's primary mission will be to understand biological threats for countermeasures and support bioforensic analysis against bioterrorism; other responsibilities include support to law-enforcement and veterinary communities. When completed in late 2008, the 160,000 square-foot facility will be the premier U.S. Biosafety Level 4 research center for biological threat characterization and bioforensic research, in two primary research areas:

:: ***Biological Threat Characterization Center*** will conduct studies and laboratory experiments to understand current and future biological threats, assess vulnerabilities to the nation, and determine potential impacts to guide the development of countermeasures against these threats

:: ***National Bioforensic Analysis Center*** will undertake bioforensic analysis of evidence from biocrimes and terrorism to determine "biological fingerprints" that identify perpetrators and determine the origin and method of attack

The **Biodefense Knowledge Center** headquartered at Lawrence Livermore National Laboratory supports collaboration and data sharing among policy makers, scientists and engineers, first responders, and other homeland security partners and stakeholders requiring timely and authoritative biodefense information.

Located on Plum Island, New York, since 1954 the **Plum Island Animal Disease Center** (PIADC) has been the first line of America's agrodefense—protecting U.S. agriculture from accidental or intentional introduction of foreign-animal diseases (FADs) into the country. Jointly operated by the S&T Directorate and the U.S. Department of Agriculture (USDA), in 2008 Plum Island is the only U.S. animal disease research facility that can provide confirmatory diagnostic capability in livestock for specific high-consequence foreign animal diseases. PIADC research programs include:

:: The ***USDA Agricultural Research Service*** (ARS) performs both basic and applied research to formulate better countermeasures, including strategies for prevention, control and recovery from FADs

:: The USDA ***Animal and Plant Health Inspection Service*** (APHIS) operates the FAD Diagnostic Laboratory, an internationally recognized lab performing diagnostic testing of livestock exhibiting clinical signs of exotic diseases

:: The ***Targeted Advanced Development*** (TAD) project brings together DHS S&T, USDA, academia and industry scientists to deliver lead vaccine and antiviral candidates for the National Veterinary Vaccine Stockpile and works with APHIS to match diagnostics to vaccines

:: The ***Disease Threat and Assessment Forensics*** unit operates a bioforensics laboratory, linked to the National Bioforensics Analysis Center, for the foot-and-mouth disease virus and other high-priority foreign animal agents

A new **National Bio-and Agrodefense Facility** (NBAF) is under development and will boast next-generation biological and defense capabilities, including the country's most-advanced biocontainment labs. Until the NBAF comes on line in 2014, upgrades to Plum Island will enable that facility to fulfill DHS S&T and USDA requirements.

The S&T Directorate's **Transportation Security Laboratory** (TSL) in Atlantic City, New Jersey, is the key U.S. government facility for test and evaluation (T&E) related to explosives and weapons-detection for all modes of transportation security. Originally established in the wake of the 1988 Pan Am Flight 103 bombing (in which 270 passengers and crew perished at the hands of terrorists), the TSL carries out T&E of transportation-security equipment, addresses future threats to the security of all modes of civil transportation and undertakes world-class research in the areas of:

- Bulk and trace sensors for explosives and weapons detection
- Human factors
- Explosives effects and survivability, including aircraft hardening
- Communications and radio-frequency identification
- Access control and analysis technology

UNIVERSITY PROGRAMS

University Programs (UP) establishes and manages the S&T Directorate's research and education outreach to U.S. universities and other institutions in close coordination with the Office of National Laboratories and Interagency and International offices. Looking to long-term U.S. homeland security S&T needs, UP nurtures partnerships with schools and universities to grow America's future scientists and engineers. And, through grants and other initiatives, University Programs contributes to the advancement of homeland security Science, Technology, Engineering and Math (STEM) education.

For example, the S&T Directorate's **Homeland Security Centers of Excellence** (CoEs) connect experts and researchers at more than 80 colleges and universities, as well as more than 20 other government agencies, industry, laboratories, "think tanks" and nonprofit organizations in collaborative workshop events.

We are establishing five new Centers of Excellence and will put in place additional CoEs in 2009 and 2010 to round-out university-based research in several critical areas:

2008 CoEs

:: Border Security and Immigration: University of Arizona and University of Texas El Paso

:: Explosives Detection, Mitigation and Response: Northeastern University and University of Rhode Island

:: Maritime, Island and Port Security: University of Hawaii and Stevens Institute of Technology

:: Natural Disasters, Coastal Infrastructure and Emergency Management: University of North Carolina Chapel Hill and Jackson State University

:: Transportation Security: University of Connecticut, Tougaloo College and Texas Southern University

2009 CoE

:: Command, Control and Interoperability

2010 CoE

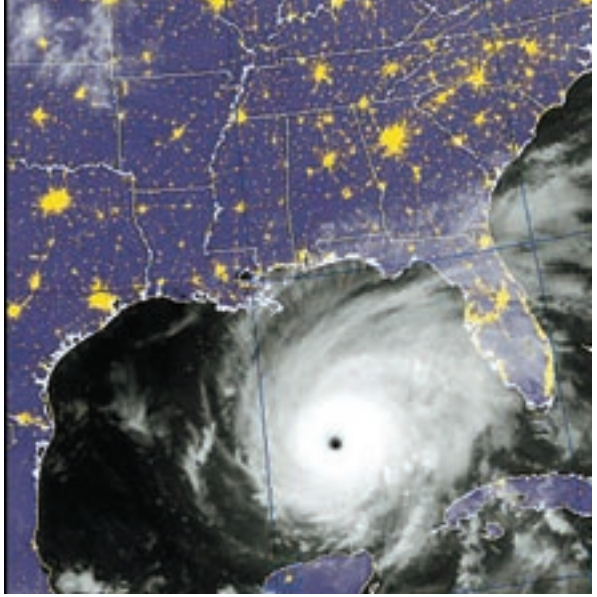
:: Chemical and Biological Countermeasures

The **Center for Advancing Microbial Risk Assessment** (CAMRA), led by Michigan State University in concert with the U.S. Environmental Protection Agency, fills critical gaps in risk assessments for decontaminating microbiological threats—such as plague and anthrax—answering the question: "How Clean is Safe?" CAMRA includes world-class scientists from Carnegie Mellon University, Drexel University, Michigan State, Northern Arizona University, University of Arizona and University of California at Berkeley, and conducts research in several vital areas: measuring exposure to biological agents in urban and natural environments; developing a methodology linking models of environmental exposure and models of disease processes to help with early detection of outbreaks, response and control efforts; producing a reference set of information on the doses and subsequent responses for specific biological agents; identifying research strategies and risk-communication priorities to improve how society manages biological risks; and developing educational programs and online learning tools to increase knowledge about microbial risk assessment.

The University of Southern California's **Center for Risk and Economic Analysis of Terrorism Events** (CREATE) evaluates the risks, costs and consequences of terrorism, and guides economically viable investments in countermeasures that will make the United States more secure. The Center comprises experts from across the country and partners with New York University and the University of Wisconsin at Madison. Among many projects, CREATE has undertaken systems analyses of nationwide border system risks and weapons threats to aviation (with a special focus on Man-Portable Air-Defense Systems, or MANPADS), risk training for Immigration and Customs Enforcement agents, economic analyses of biological risks and radiological attacks on ports, and decision analysis of terrorist preferences for weapons types and targets. Overseas, CREATE has linked with an Israeli organization to address peroxide-based explosives.

The **National Center for Foreign Animal and Zoonotic Disease Defense** (FAZD) led by Texas A&M University, researches the introduction of high-consequence foreign animal and zoonotic diseases into the United States, with an emphasis on prevention, surveillance, intervention and recovery. Core FAZD members include the University of California, Davis; the University of Southern California; and the University of Texas Medical Branch. Among numerous efforts are: development of new methods for rapid and accurate detection of foot-and-mouth disease, rift valley fever and avian flu; research into new vaccines and anti-viral agents to protect animals from introduced diseases; and developing approaches to curtail spread of diseases.

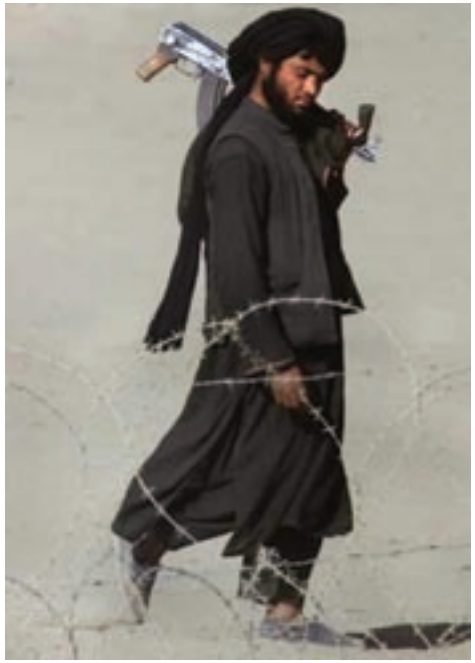
The **Discrete Sciences Centers** (DSC) are led by Rutgers University, the University of Southern California, University of Illinois at Urbana-Champaign and the University of Pittsburgh. These organizations collaborate with the Institute for Discrete Sciences at Lawrence Livermore National Laboratory to conduct research on advanced methods for information analysis and the development of computational technologies to protect the country. Key activities and accomplishments include development of an information-extraction data-mining system that can process text articles about infectious disease outbreaks world wide and identify the diseases and victims; an Internet/Web-based system that associates keywords to geospatial databases such as maps, satellite and aerial imagery; and developing external memory algorithms clusters for visualizing larger graphs connected entities of interest—people, organizations, organizations, events, documents and the like—and rapidly identifying patterns in graphs that are too large to fit within a computer's main memory.



The **National Center for Food Protection and Defense** (NCFPD), led by the University of Minnesota, protects the food system—from pre-farm inputs through consumption—by establishing best practices, developing new tools and attracting new researchers to prevent, manage and respond to food-contamination events. Efforts include development of a prototype food-event modeling system, realistic decontamination protocols using surrogate agents and food matrices, and risk-communications approaches to minimize the public impact of food contamination events. In response to several contamination events in 2006-2007, NCFPD researchers analyzed food ingredients and products imported from the People's Republic of China. The center also helped to identify foods and ingredients needing increased scrutiny on the basis of assessed vulnerabilities and limited opportunities for substitutes.

The **National Center for the Study of Preparedness and Catastrophic Event Response** (PACER), led by the Johns Hopkins University, optimizes America's readiness in the event of a high-consequence natural or man-made disaster and develops guidelines and best practices to alleviate the effects of such an event. The PACER team includes the Brookings Institution, Florida State University Consortium, Morgan State University, University of Alabama and University of Buffalo. Key projects include: developing tools to assess risk-readiness for catastrophic events; improving the response capabilities of agencies and first responders through wireless networks of sensors, remote cameras and magnetometers; and identifying communications and data-fusion techniques to improve situational awareness and critical decision-making capabilities.

The **Regional Visualization and Analytics Centers** (RVACs) comprise the Penn State University, Purdue University, Stanford University, University of North Carolina at Charlotte and University of Washington. In close collaboration with the National Visualization and Analytics Center at the Pacific Northwest National Laboratory, the RVACs undertake far-reaching research on visually based analytic techniques that help people gain insight from complex, conflicting and changing information, for example: GeoDiscover is a tool for geographic contextualization of documents and geospatial information to identify and map social networks; FactXtractor extracts entities, locations, times and concepts from text and has been used to create FEMARepViz, a tool to visualize daily FEMA situation reports; and WireVis, a highly interactive visual analytical tool to help detect and track suspicious financial wire-transfers, i.e., suspected money laundering by drug cartels and transfer to terrorist organizations.



The **National Consortium for the Study of Terrorism and Responses to Terrorism** (START), led by the University of Maryland, informs decisions on how to disrupt terrorists and terrorist groups, while strengthening the resilience of U.S. citizens to terrorist attacks. Projects include the development of the world's largest and most up-to-date databases of the more than 85,000 terrorist events since 1970; developing tools and data on the "life cycle" of terrorist groups, terrorist group information and terrorist capabilities; identifying groups within the United States most vulnerable to the effects of a terrorist act; and assessing nationwide community preparedness for terrorist events. START has also looked overseas for solutions, for example, collaborating with King's College in London and Sweden's National Defence College to analyze group radicalization.

As American education pioneer John Dewey understood, "Education is a social process. Education is growth. Education is not a preparation for life; education is life itself." The University Programs' Science, Technology, Engineering and Math education initiatives embrace that philosophy to attract and develop today the scientific leadership needed for tomorrow. These programs are strengthening the expertise and diversity of our S&T workforce in the STEM arenas through support to DHS-related curricula and programs at a broad spectrum of academic institutions and research facilities and high-performing students. The S&T Directorate's scholarships and fellowships link explicitly to the six S&T technical divisions and the Centers of Excellence:

:: The Scholarship and Fellowship Program provides scholarships and fellowships to individuals in support of undergraduate and graduate students who are pursuing degrees related to homeland security S&T needs

:: The HS–STEM Career Development Grants Program funds grants to institutions to underwrite scholarships and fellowships to undergraduate and graduate students who are pursuing degrees related to homeland security S&T needs

:: The Visiting Scholars Program gives opportunities for faculty and university researchers to work closely with professionals at a DHS or national lab for up to two years

:: The Summer Internship Program provides undergraduate juniors and seniors the opportunity to work with homeland security researchers at federal laboratories and research institutions

:: The DHS Post-Doctoral Program provides opportunities for post-doctoral research to extend or expand areas of knowledge critical to homeland security

University Programs also has developed significant engagements with Minority-Serving Institutions (MSI). The MSI Scientific Leadership Grants combine early career financial support to promising researchers who are working in homeland security-related STEM disciplines. UP supports a Summer Research Team Program for faculty and student research teams from Historically Black Colleges and Universities, Hispanic Serving Institutions, Tribal Colleges and Universities, and Alaska Native and Native Hawaiian Serving Universities to conduct research at DHS Centers of Excellence. The MSI Summer Research Team Program enhances the scientific leadership at MSIs by providing meaningful research opportunities to highly talented and diverse individuals in research areas that support America's security needs. University Programs also sponsors a one-week Summer Workshop on Teaching Terrorism for MSI faculty.

In all these ways the S&T Directorate draws upon the RDT&E capability across all elements of the Homeland Security Research Enterprise in the United States and throughout the world to deliver the products and services that our DHS customers and first responders desire and deserve.

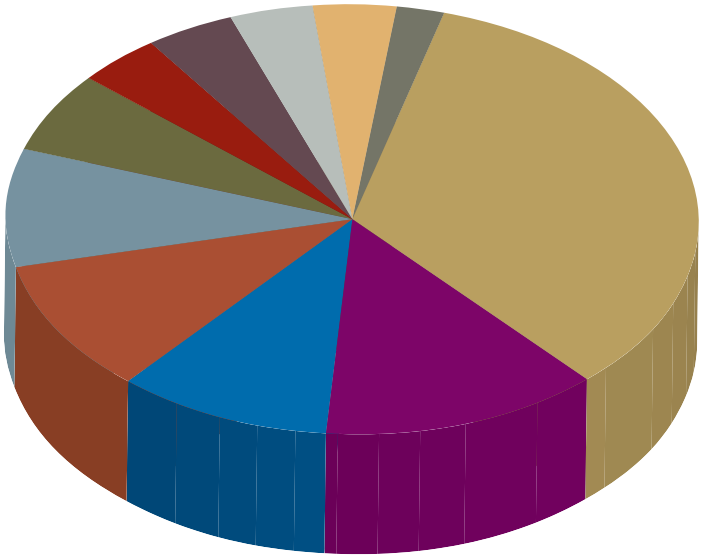
In the War on Terrorism, America's principal advantage is its unparalleled technological superiority—measured not only in highly sophisticated hardware and software—but also in the competence and character of its citizens in controlling that technology.

Report of the Committee on Commerce, Science and Transportation
April 2002

FOUR :: DELIVERING RESULTS

The S&T Directorate has several hundred individual projects under way and planned in 2008, focusing the imagination, enthusiasm and perseverance to enhance America's security against acts of terrorism and other disasters. We have provided here overviews of just a few of the projects that will deliver game-changing products and services to meet our DHS customers' and first responders' needs—making America a safer place…enabling life, liberty and the pursuit of happiness.

The allocation of RDT&E funding to the Innovation/HSARPA Office, the six technical divisions and throughout the Homeland Security S&T Enterprise evolves from year to year in response to our assessments of the threats, challenges and requirements, but we always are mindful of the fundamental need for good stewardship of the nation's resources.



- Chemical & Biological :: 35%
- Laboratories :: 14%
- Explosives :: 10%
- Command, Control & Interoperability :: 10%
- Innovation/HSARPA :: 9%
- University Programs :: 6%
- Borders & Maritime :: 4%
- Test & Evaluation/Standards :: 4%
- Transition :: 4%
- Infrastructure & Geophysical :: 4%
- Human Factors :: 2%

(May not total 100% due to rounding.)

FISCAL YEAR 2008 DHS S&T FUNDING ALLOCATION

EXPLOSIVES

Explosives and other volatile materials are the weapons of choice for terrorists plotting to disrupt daily life and create mass casualties and broad swaths of destruction. The S&T Directorate Explosives Division focuses on innovative approaches in detection, response and mitigation to protect our citizens and America's infrastructure from non-nuclear explosives and other "energetic" threats.

The need to detect or defeat explosive devices surreptitiously brought on board aircraft is a national priority. Begun in 2006 in collaboration with the DHS Transportation Security Administration (TSA), the **Air Cargo Explosives Detection Pilot Program** is testing new technologies and concepts of operation for a significant effectiveness increase in screening air cargo, generally, and enhancing the probabilities of detecting explosives and stowaways. T&E of prototype cargo-handling and -screening systems, including **Explosive Trace Detection** tools and a dedicated **Explosives Detection System**, continues and, once on line, will significantly increase our ability to defeat these threats.

Similarly, the terrorist bombing at the Altanta Olympics in July 1996, which killed two people and injured more than 100, tragically underscored the threat from the lone bomber in crowds. The **Checkpoint Explosives Detection Program** is developing portable, standalone screening systems for people and personal items at special events as well as mass-transit locations. The program's goals are high-throughput screening with minimum false-alarm rates, increased system availability and reliability, reduced costs and reduced retention time during non-intrusive personal searches. We continue testing integrated systems capable of detecting explosives—including gel-based and liquid materials and homemade explosives under the **Magnetic Resonance Imaging Rapid Liquid Component Detector Project**—and handguns to provide early warning of a suicide bomber attack. In early 2008, we are carrying out proof-of concept assessments to deliver a prototype portal for TSA evaluation later this year.

The objectives of S&T's **Standoff/Remote Detection Program** are, first, to provide a standalone IED detection capability against suicide bombers, vehicle-borne IEDs or leave-behind bombs, and, second, to develop hand-held systems and mobile screening stations that can be rapidly deployed and remotely operated in a layered-security architecture. The 2004 Madrid train bombing that killed 191 people and the 2005 London subway and bus attacks that killed 52 tragically underscored the need to discern quickly and accurately the distinguishing features of explosives and explosive devices to identify the suicide bomber but not impede the lawful movement of private and commercial traffic—personal privacy and safety are always vital considerations. Efforts focus on baseline performance demonstrations of enhanced sampling techniques, such as non-intrusive spectroscopic and highly selective trace detection, magnetic and vibration anomaly imaging for short-range standoff detection and mechanical property sensing.

A menace to global aviation, more than 500,000 Man-Portable Air Defense Systems—shoulder-launched anti-aircraft missiles—are in world inventories and many thousands are on the black market and available to terrorists on a cash-and-carry basis. These weapons have already been used for terror, at least since the 1970s. In September 1978, for example, an Air Rhodesia passenger airliner crash-landed after being struck by a MANPADS fired by Zimbabwe Peoples Revolutionary Army rebels, killing 32 passengers. The **Counter-MANPADS Program** focuses on two means to defeat these weapons: (1) aircraft-borne Directed Infrared Countermeasures (DIRCM); and (2) non-DIRCM airborne and ground-based Emerging Counter-MANPADS Technology (ECMT) countermeasures. The DIRCM program is modifying and evaluating Department of Defense technology for its applicability in the commercial aviation environment. Live-fire tests of the two certified DIRCM systems began in the fall 2007 at the White Sands Missile Range, and the Explosives Division will also conduct a passenger aircraft service evaluation to complete in FY 2009. The ECMT program began in FY 2007 and is examining forward-leaning concepts to determine their potential suitability and interoperability in the civilian aviation environment; it will conclude in late 2008.

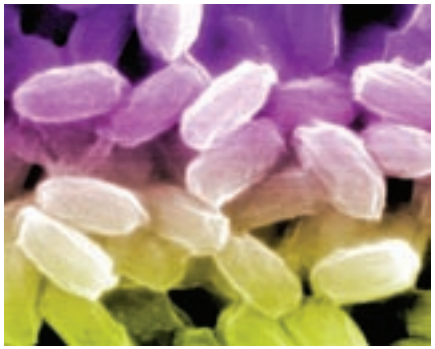
The Explosive Division is also investigating the feasibility of an airborne, persistent standoff MANPADS countermeasures system comprising one or more high-altitude, long-endurance Unmanned Aircraft Systems (UAS) fitted with Missile Warning System (MSW) and MANPADS countermeasures stationed in commercial airspace above airports. The goal of **Project CHLOE** is to achieve autonomous coverage and protection for all aircraft within local MANPADS threat envelopes through real-time sensor-fusion and data-dissemination. The program will also investigate and demonstrate other DHS missions and payloads that are compatible with the CHLOE technology platform, including emergency and disaster-relief communications-relay support; border and coastal security for surveillance, detection, identification, and cueing; and critical infrastructure monitoring. In FY 2008, we will modify a DoD Missile Warning System for UAS application and demonstration; efforts in FY 2009 will demonstrate high-altitude missile warning and nullification.

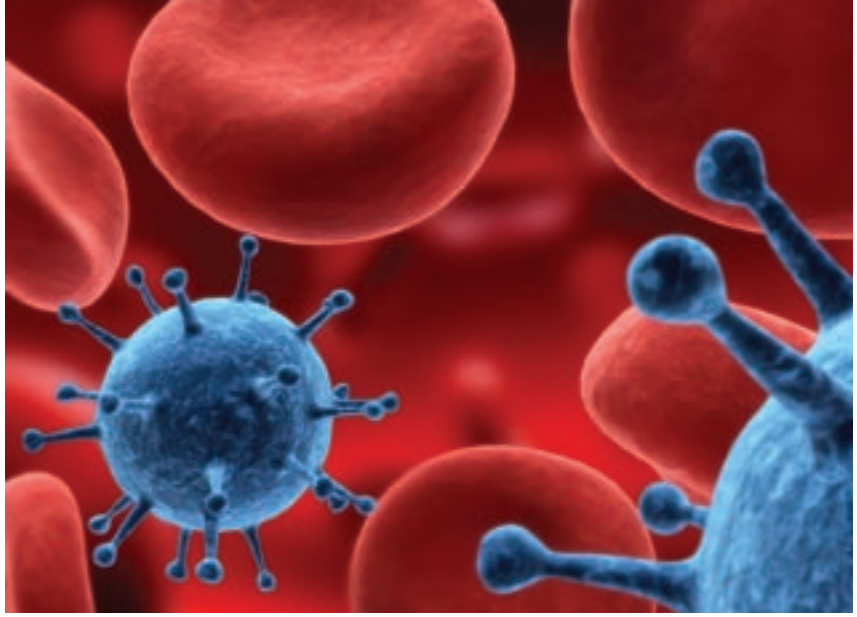
CHEMICAL AND BIOLOGICAL THREATS

In his *Biodefense for the 21st Century*, the President stated, "Biological weapons in the possession of hostile states or terrorists pose unique and grave threats to the safety and security of the United States and our allies…. The stakes could not be higher for the nation." The National Research Council report *Making the Nation Safer* concluded, "chemicals continue to be the weapon of choice for terrorist attacks. They are readily available and have the potential to inflict significant casualties…." With these threats in mind, the Chemical and Biological (Chem/Bio) Threats Division supports science and develops technology to reduce the probability and potential consequences of a biological or a chemical attack on our civilian population, infrastructure or agricultural systems. The Division conducts focused RDT&E efforts in five critical thrust areas: Threat Characterization and Awareness; Surveillance and Detection; Forensics; Response and Recovery; and Agrodefense.

The **Threat Characterization and Awareness Program** provides enhanced understanding of current and future biological and chemical threats and conducts risk assessments across the broad range of threats. These risk assessments help prioritize the threats that pose the greatest risks and explore countermeasures offer the greatest protection. The program also carries out population threat assessments under the BioShield Act of 2004 to support the Department of Health and Human Services' prioritization of medical countermeasures.

On 20 March 1995, members of the Aum Shinrikyo cult entered the Tokyo subway system and released the deadly nerve agent Sarin in a coordinated, simultaneous, multi-target attack that killed 12 people and injured another 3,800. The specter of such attacks in the United States has focused the chemical portion of the **Surveillance and Detection Program** on advanced warning and notification of a chemical threat release and technologies first responders need to survey potentially contaminated scenes while limiting their exposure to chemical warfare agents (CWAs) as well as more common toxic industrial chemicals (TICs). Current systems are unable to detect a wide range of CWAs and TICs with the low false alarm rates needed for facility and first-responder protection—challenges that demand a leap forward in technology for next-generation systems. The program is developing technologies that in a single package can accurately detect CWAs and TICs, focusing on three major detection systems: (1) Autonomous Rapid Facility Chemical Agent Monitor for continuous monitoring of facilities; (2) Lightweight Autonomous Chemical Identification System for use by first responders; and (3) Low-Vapor Pressure Chemicals Detection Systems. Once deployed, these systems will provide early detection and warning to potential victims and first responders.





In the fall 2001, letters containing anthrax spores were sent to U.S. organizations and political offices, bringing government and commercial operations from Florida to Connecticut to a halt, killing five people and infecting another 17. The crime remains unsolved, but the possibility of future, larger and more indiscriminate bio-attacks continues to motivate the **BioWatch Program** to provide "24/7/365" bio-terrorism detection systems in more than 30 of the top threat cities across the country. In partnership with the Environmental Protection Agency and the Centers for Disease Control, in 2003 DHS S&T deployed the Gen-1 BioWatch system, which can detect and analyze Biological Threat Agents (BTAs) in 12-36 hours. The completion of the Gen-2 enhancements in 2007 provides better spatial coverage and an indoor detection capability in the nation's top-ten threat cities. The fully autonomous next-generation system, now in development, will significantly expand existing coverage of the U.S. population, increase the number of BTAs detected and reduce detection times to three to six hours, and at the same cost as the in-service BioWatch system. By providing early detection of an attack, BioWatch can speed the decision to deploy medical countermeasures, thereby greatly reducing casualties. It will also play a key role in reassuring the public as to whether or not there has been a follow-on attack. BioWatch technology-development efforts are complemented by efforts to develop real-time biological agent detection systems that can detect biological agents in five minutes or less. These detection systems can then serve as biological "smoke alarms" for protecting public facilities, such as transportation hubs, sports arenas and high-value government and corporate buildings—a positive signal can trigger various actions, from turning off the forced airflow in a facility to total evacuation.

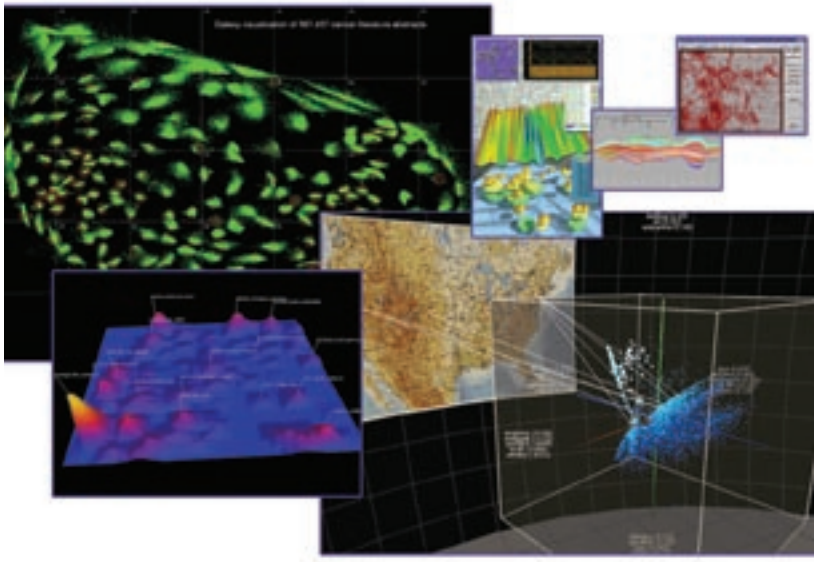
In invent of an actual biological or chemical event it will be important to identify the perpetrator as quickly as possible to prevent follow-on attacks. The **Forensics Program** conducts technical analyses of samples to help provide indications to how, where and when the sample may have originated. These forensic analyses are performed in close coordination with the Federal Bureau of Investigation, and the results are used to support investigations. In addition to this operational forensic role, the division conducts RDT&E on next-generation forensics tools including: improved sample preservation methods for integrity, stability and viability; understanding of molecular markers for identification and comparative analysis; improved extraction of genomic material from complex matrices; improvements in fundamental knowledge of the physical and chemical properties of the carrier matrix; bioinformatic tools for *in-silico* modeling of molecular markers; and tools for rapid "rule in/rule out" of evidence.

And, in partnership with the U.S. Department of Agriculture, the **Agrodefense Program** plays a significant role in defending against the natural as well as intentional introduction of foreign animal diseases into the country. The program has a major role in leading the expansion of current and new agricultural countermeasures and developing a plan to provide safe, secure, state-of-the-art biocontainment laboratories for researching FADs and zoonotic diseases. The program supports the Plum Island Animal Disease Center and planning for the future National Bio-and Agrodefense Facility. Vital activities include development of next-generation veterinary vaccines and biotherapeutics to mitigate the spread of an outbreak, high-throughput diagnostics to guide the responses and models of disease spread and economic impacts to inform decision makers in the identification and selection of various intervention strategies. These will be vitally important for detecting and containing outbreaks of FADs and for minimizing their impact on U.S. foreign trade.

COMMAND, CONTROL AND INTEROPERABILITY

A lesson learned and relearned is the need for "scaleable, seamless, secure connectivity" among emergency-response agencies and personnel. Effective "C-Cube"—Command, Control and Communications—depends on a broad spectrum of interoperable and compatible technologies, architectures, protocols and systems for information management and sharing, situational awareness and cyber security. The goal is to enable multiple disciplines and jurisdictions to exchange voice, video and data on demand, and assure a real-time common operational picture that is critical to mission success. Protecting sensitive computer systems from cyber attack is also a fundamental objective. The S&T Directorate's Command, Control and Interoperability Division (CID) and the division's Office for Interoperability and Compatibility focus RDT&E efforts in five thrust areas—Basic/Futures Research; Communications, Interoperability and Compatibility; Cyber Security; Knowledge Management Tools; and Reconnaissance, Surveillance and Investigative Technologies—to meet these critical needs.

The **Visual Analytics and Physics-based Simulation Program** carries out basic research on novel advanced technologies and techniques for visually based analytical processes and physics-based simulations. The program focuses on computer-, algorithm- and network-efficient methods for interacting with, understanding and sharing heterogeneous data from diverse, diffuse and distributed sources in real time. The goal is to enable rapid, visually driven decision-making techniques and common operating pictures for proactive threat assessment and effective and timely disaster and incident response to prevent terrorist incidents and protect the homeland from natural or man-made catastrophes.



CID's **Standards and Modeling Program** focuses on voice and data standards for interoperability and information sharing. Major efforts focus on the development of communications and data messaging standards—including the "Project 25" suite of standards, the Common Alerting Protocol, the Distribution Element, the Hospital AVailability Exchange (HAVE) and Resource Messaging—that enable emergency information sharing. During 2008-2009, we will develop and test model broadband standards, expand messaging standards to work seamlessly with the health field in emergency-related exchanges, demonstrate Voice over Internet Protocol (VoIP) gateways and develop a compliance-assessment program to ensure industry implementation of standards in applicable commercial products. The results will be enhanced interoperability and compatibility of communication systems regardless of manufacturer, operational flexibility and agility, shortened response time, and reduced errors and confusion during response and recovery efforts.

The DHS **Cyber-Security Experimental Research Test Bed Program** provides a test bed isolated from the live Internet but with sufficient topological complexity to emulate a scaled-down but functionally accurate representation of the hierarchical structure of the real Internet and to approximate the real-world mixing of benign traffic and cyber-attack traffic for tests of cyber-related R&D technologies before they transition to operational environments. This program specifically addresses the need to increase capability for experimentation and testing of cyber-security defense technologies and to enhance situational awareness for increased security, especially for Supervisory Control and Data Acquisition (SCADA) systems at petroleum refineries and other large industrial facilities.

Linked to the Experimental Research Test Bed efforts, CID's **Research Data Repository Program** provides real-, network- and system-traffic datasets that researchers can use to validate their technologies and products for cyber security, before the technologies and products are deployed online. Through 2007, more than 50 technologies had been tested, and by the end of 2008 CID will increase the capacity of the cyber security test bed to more than 800 systems, 150 large-scale datasets and 250 dataset applications, which will support 85 test-bed users and some 1,600 large-scale, malicious-code experiments per month. Another 1,500 data sets will be delivered during the next several years to enable continued testing and evaluation of new cyber-security threats and support delivery of new security capabilities.

The division's **Architecture and Framework Program** develops and deploys technologies to analyze masses of data in different formats and types, from different sources, with varying degrees of confidence levels and within critical timeframes required for rapid decision-making. The program includes several projects at the U.S. Computer Emergency Readiness Team (US-CERT) and the Datacube and Pronet projects at Immigration and Customs Enforcement. The program has three principal goals: (1) provide intelligence analysts with tools to "connect the dots" with information not previously considered together or relevant; (2) identify and locate high-value documents from huge data streams; and (3) enable analysts to share information and understand threat pictures and hypotheses. Through 2007, CID had deployed two new technologies, and the division plans for two new deployments each year to DHS components. The results will be vastly improved knowledge-management tools for emergency-response decision makers and emergency-response people in the field.

BORDERS AND MARITIME SECURITY

The Borders and Maritime Security Division (BMD) develops and transitions technologies and tools that improve the security of America's land and maritime borders and ports of entry without impeding the flow of legal commerce and travelers. With the ultimate goal of stopping threats before they enter the United States, BMD carries out numerous programs in two thrust areas: Border Watch, which comprises the Border Technologies, Maritime Technologies, and Border Officer Tools and Safety programs to increase detection of illegal border activity, reduce manpower, improve agent response times and increase officer safety; and Cargo Security, which operates through the Cargo and Conveyance program to develop technologies and systems that ensure the integrity of cargo shipments—particularly the millions of shipping containers that pass through land and sea ports of entry each year—and enhance the end-to-end security of the supply chain. BMD's key projects include:

Such programs as CPB's **Secure Border Initiative Network (SBInet)** and the **Coast Guard's Command 21 Project** will develop, integrate and test sensor technologies in an operational environment, providing in-the-field capabilities to improve mission effectiveness and agent safety. The project includes several efforts: (1) the BorderTech Testbed for the evaluation of capabilities—Geo-Spatial situational awareness, biographic/biometric detainee background checks, multi-sensor integration, and wireless connectivity—to enhance agent training and tactics development; (2) Advanced Sensor Technologies that focus on unattended ground sensors, fiber-optic cables, fence sensor algorithms, electro-optical/infrared devices, airborne systems and advanced sensor processing; (3) the Advanced Ground Surveillance Radar effort for active and passive technologies (e.g., multi-static, foliage-penetration and ultra-wideband) to detect and continuously track humans at distances up to ten miles; and (4) Tunnel Detection takes a broad-spectrum approach to defeating illegal border activities underground. The results will be increased border agent safety and improved response times; increased detection, tracking and apprehension rates; and reduced technical risk and acquisition and in-service costs.

The **CanScan** and **SAFECON** (Safe Container) Projects address S&T's highest cargo-security capability need to enhance cargo container screening and examination systems. The CanScan project looks at alternative technologies to existing Non-Intrusive Inspection (NII) systems to provide a mobile and interoperable capability with increases in reliability, penetration, resolution and throughput. The goal is to be able to detect and identify concealed contraband items (e.g., drugs, money, illegal firearms, WMEs and explosives) and humans through NII methods. An automatic target recognition capability will also be integrated into the CanScan system. Additionally, the capabilities developed will be applicable to air cargo security. SAFECON is a crane-mounted sensor system that interrogates

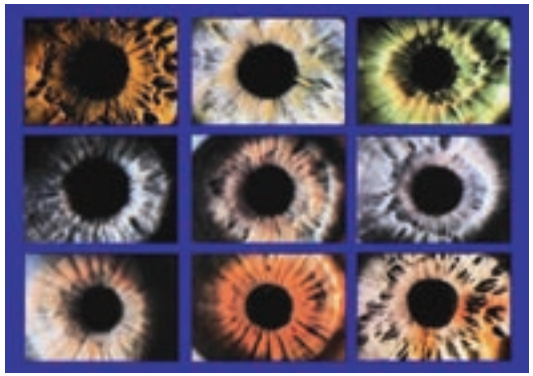
shipping containers and detects and identifies dangerous cargo (chemical/biological agents, explosives and human cargo) during normal ship load/unload operations. CanScan and SAFECON are complemented by the **Advanced Container Security Device** (ACSD) Project, which is developing an advanced sensor system for monitoring six-sided container integrity and to detect the presence of humans in the container. If ACSD detects an intrusion, breach, door opening or a human, it will transmit alarm information through the Marine Asset Tag Tracking System (MATTS) to Customs and Border Protection. The ACSD will also have an open-architecture interface capability to integrate future sensors (e.g., chemical/biological) as they are developed. In 2008, we will receive 40 ACSD prototypes with integrated MATTS global communications for prototype system testing in 2008 and 2009.

The **Sensors and Surveillance Project** involves visual and non-visual technologies to monitor vessels, objects or processes along maritime borders for conformity to expected or desired norms: (1) Affordable Wide-Area Surveillance Capability for detection, tracking and classification of vessel traffic; (2) Advanced Geospatial Intelligence Technical Exploitation for wide-area surveillance of the offshore maritime environment; (3) Port and Coastal Radar Improvement prototype radar system enhancement for harbors, waterways and offshore areas; (4) Offshore Deepwater Buoy and Vessel Tracking Program Pilot comprising deep-water buoys for detection and classification of non-cooperative vessels; (5) Assess Mission Enhancement via Near-Space Systems using space assets and sensors; (6) Port/Harbor Underwater Change Detection and Hull Inspection technologies for surveying underwater areas and vessel hulls to detect anomalies, such as underwater IEDs and limpet mines; and (7) the Small Boat Harbor Surveillance Study/Pilot effort for tracking small boats in port environments. Once deployed, these capabilities will significantly enhance U.S. Maritime Domain Awareness and response capabilities.

The **Sensors/Data Fusion and Decision Aids Project** is developing the systems for a significant enhancement to multi-agency law-enforcement decision-making, coordination and execution. The project's goals include the capability to fuse tactical information from multiple data sources, to generate real-time situational awareness and to identify and track high-risk targets (people/vehicles/vessels) automatically. The western Lake Erie pilot effort, NorthGuard, demonstrated the operational utility of coupling advanced sensor-fusion and tracking technologies with a common operational picture. In FY 2007, the project conducted the **Northern Border Maritime Data Fusion/Situational Awareness Pilot** with good results. These efforts have provided insight into operational issues, such as the effectiveness of the Trusted Traveler program and whether other individuals are reporting arrival in the United States as required. In FY 2008, the project is testing the Automated Scene Understanding toolset designed to improve efficiency and effectiveness of watchstanders and agents by autonomously detecting prohibited, suspicious and anomalous behaviors based on system self-learning or operator-generated rules.

The **Border Officer Safety Project** plans to integrate technologies that will enable border security law enforcement agents to perform their missions safely, including: (1) Enhanced Ballistic Protection for lighter-weight, more durable and higher-strength materials and equipment that also reduces equipment load; (2) Automatic Facial Recognition, which captures images of individuals and compares them to law enforcement databases; (3) Hidden Compartment Inspection Device, for non-intrusive detection from greater stand-off ranges of humans and contraband hidden behind walls and other barriers; and (4) Pursuit Termination-Vehicle/Vessel Stopping, a user-safe, non-lethal means of stopping uncooperative vehicles and vessels.

HUMAN FACTORS



Terrorists are human, and terrorism is behavior—as are our responses to catastrophic events. The Human Factors Division (HFD) applies social and behavioral sciences to deliver results in several critical areas: (1) accurate, real-time credentialing and biometrics capabilities to identify terrorists and criminals at access-control points for U.S. air, land and sea borders and critical infrastructure; (2) hostile-intent detection capabilities to spot deceptive and suspicious behavior in individuals; (3) understanding the analytical, operational and policy concerns related to terrorist activities; (4) insight into the psychological, social and economic impacts of catastrophic events to enhance the government's and the public's ability to prepare for, respond to and recover from disasters; and (5) a Human-System Integration (HSI) process and principles that integrate human-performance considerations into all stages of S&T RDT&E to optimize total system performance and ownership costs.

The **Biometrics Program** is developing multi-modal—finger, face and iris—real-time, contactless biometric tools to improve the accuracy of screening for individuals of interest. In FY 2008 we will initiate efforts to develop improved biometric collection devices and the establishment of a framework for a usable multi-modal integrated biometric system. Subsequent efforts will assess these devices within the initial framework to determine their level of improved performance. This will deliver real-time, positive and accurate biometrics-based identification of known terrorists prior to their entering the country and increase the throughput of travelers across U.S. borders—vital capabilities to enhance security.

As a means to increase screener threat detection performance, the **Enhanced Screener-Technology Interface Project** addresses the integration of human-in-the-loop technology systems used by transportation screeners. This project increases the effectiveness and efficiency of transportation screening systems, decreases physical stress and fatigue, and reduces human error in the screening process. Primary research topics focus on improving the interface, the display and operator procedures. Activities include the development and enhancement of technology controls that match the cognitive, perceptual and physical abilities of human operators. Additionally, the project addresses novel, human-systems integration approaches to optimize display images so that the images correspond with operators' individual attention spans and perception abilities. Finally, we are examining operating procedures to ensure they match human cognition, reasoning and attentional processes. This project proposes new screener technologies and procedures and develops training curricula to optimize security effectiveness and reduce human fatigue and injury, while reducing training requirements and overall cost. Another current objective is to develop a standard display that is consistent across vendors and varying technologies, which will minimize training requirements, provide more consistent image interpretation and increases throughput. We are, as well, developing new training procedures for visual-search tasks (e.g., checkpoint explosive-detection systems and X-ray).

Understanding our adversaries is fundamental to our security. **The Group Violent Intent Modeling and Simulation Project** analyzes and models terrorist behavior to understand the threat and to increase our ability to assemble and test competing scenarios as terrorist-related events unfold in real time. This project will develop a computerized intelligence analysis framework that extracts information about the indicators of terrorist intentions, estimates future terrorist behavior based on social and behavioral sciences, and models and simulates various influences on future behavior. Last year, we delivered Version 1 of a baseline terrorist group-level modeling and simulation capability and completed an integrated group-level analytical framework and system. In FY 2008, we will complete and implement Version 2 of the system, and in FY 2009 we will complete our modeling capabilities and content analysis and information-extraction system and will deliver the final version the next year. Subsequently, we will complete a similar effort aimed at radical movement intent modeling.

There is a compelling need for a non-invasive capability to monitor individuals traveling into and out of the United States, enabling us to identify and track unknown and potential threats, without constraining lawful activities or decreasing the throughput of legitimate travelers and commerce across U.S. borders. The **Hostile Intent Detection Automated Prototype Project** is developing a real-time, multi-modal, culturally independent and non-invasive hostile-intent screening and detection prototype—focusing on behavioral cues—with an initial 75 percent accuracy rate. This project will demonstrate real-time automated intent detection in FY 2009. That year, we will also transition expanded, multi-cultural intent indicators, and in FY 2012 we will transition a multi-modal automated intent-detection capability. Subsequent efforts will see: (1) transitioning of culturally neutral intent indicators; (2) demonstration and transition of culturally neutral validated and reconfigurable automated intent detection; and (3) delivery of engineering tradeoff studies.

A related effort is the **Cross-Cultural Validation of SPOT Project**, which addresses the need for enhanced capabilities for detecting suspicious behavior through multi-cultural, validated observational techniques that can be employed before a person commits a hostile act. DHS S&T is analyzing current operational protocols to give customers a better understanding of the indicators of hostile intent and is establishing protocols to enable cross-cultural validation of behavioral indicators. The cross-cultural training and indicators will be integrated into current SPOT training programs. By FY 2011, we will have integrated the cross-cultural indicators into Stand-Off Hostile Intent Training courseware, evaluated the resulting training effectiveness gains and delivered a complete cross-cultural SPOT course.

Catastrophic events have dramatically underscored the need for the government to improve public/private preparedness, response and recovery. The **Risk Perception, Public Trust and Communications Program** establishes baselines and recommendations for government communications strategies, plans, programs and operations during catastrophic events so that affected communities can better prepare for, respond to and recover from such events. During the next two years, HFD will identify effective messaging for diverse and multi-cultural populations, quantify the impact of this messaging, identify effective media for dissemination, and determine the most effective messaging strategies and content. We will subsequently assess the differential impact of messaging on diverse/multi-cultural audiences, determine the most effective media for communicating to these audiences, identify the most effective level of the populations toward which to direct the messaging, and analyze and determine how effective messaging differs during the various phases of an event—all to improve the public's safety and security.

INFRASTRUCTURE AND GEOPHYSICAL

Protecting the country's critical infrastructure requires all-hazard preparedness, response and recovery at national regional, state and local levels of concern. The S&T Directorate's Infrastructure and Geophysical Division (IGD) focuses on providing superior situational awareness, improved emergency-responder capabilities and critical infrastructure protection across numerous activities in three primary thrust areas: (1) Critical Infrastructure Protection focuses R&D activities in the 17 Critical Infrastructure/Key Resource sectors; (2) Preparedness and Response develops and deploys capabilities to improve preparedness, response and recovery from all-hazards emergencies: and (3) Geophysical develops technologies and systems to address America's geophysical concerns—including hurricanes, floods and earthquakes.

The **Protective Technologies Program** is developing revolutionary capabilities to protect America's most vital critical infrastructure assets primarily against blast loads and effects, such as shrapnel from weapons and flying debris fragments formed by blast and fire. The goal is to enable owners and operators to implement effective, affordable and reliable materials and design procedures and to establish innovative construction methods to reduce the risk to critical infrastructure assets.

During FY 2007, the program began physical testing and numerical modeling of blast effects on embankment dams and mitigation measures for tunnels and bridge cables. In 2008, the project will evaluate blast effects and mitigation measures for dams, tunnels and bridges. In 2009, we will identify new materials, the appropriate scale of materials and the appropriate types of numerical analysis codes needed to model these materials at the molecular level. We will continue basic research in these areas and will mature the protective measures for tunnels, begin development of protective measures for additional classes of vital critical infrastructure and conduct field experiments of the existing and new prototype protection for tunnels.

About 60 percent of America's gross domestic product is directly tied to electric power, and the U.S. power-generation and transmission system today is operating at capacity. It is, moreover, a "soft target" for terrorist attack and can be vulnerable to natural disasters and man-made events, resulting in black outs, brown outs, rolling outages and cascading failures. The August 2003 outage, for example, cost the U.S. economy approximately $10 billion and left some 50 million people and many thousands of businesses in the dark. Much of the existing electric grid is highly susceptible to brown outs and black outs, and current methods for preventing power outages and restoring power are often costly and slow and require extraordinary efforts. Existing technologies and planned mitigations also require a great deal of space, which is problematic in dense urban areas. The **Resilient Electric Grid (REG) Project** addresses these concerns and will protect critical, electric power-dependent infrastructure from the cascading effects of a power surge on electrical grids. This project will demonstrate key components of a future "micro-grid" that will instantaneously reduce power surges and allow for multiple alternative pathways of power delivery, providing resilience against natural disasters and deliberate attacks. Such capabilities could save on the order of $100 billion per year—$1 billion in New York City, alone—in losses from normal events, and would help prevent devastating—potentially many hundreds of billions of dollars—impacts from catastrophic natural events and deliberate attack, and thus contribute to inherent deterrence. The project's first major achievement in 2008 was the successful laboratory proof-of-concept demonstration of a fault-current limiter high-temperature superconducting (FCL HTS) cable that was able to transmit power with no electrical losses and simultaneously prevent cascading failures. This success indicates that FCL HTS cable enables an innovative grid architecture that will act as a system of resilient power distribution pathways with built-in circuit breakers. The project will continue to demonstrate key supporting technologies in laboratory and representative environments preparation for prototype deployment in the Manhattan electric grid in 2010.

Hurricanes can generate extreme storm surge and wave conditions for several hundred miles, while flooding associated with the hurricane surge—even without wind and wave effects—can be widespread. Katrina produced devastating surge and wave conditions for the entire east-facing levee system of southeast Louisiana and the entire coast of Mississippi, some 200 miles in length, while storm-surge and wave action were felt miles inland, in some cases completely destroying entire city blocks. The S&T Directorate's **Hurricane and Storm-Surge Mitigation Project** is exploring non-traditional solutions to complement traditional engineering—permanent levees, seawalls, gates or other permanent closure features. The division is assessing natural landscape features—wetlands, coastal ridges, barrier islands and reefs, vegetation buffers—and short-term, local interdiction tools—temporary low-cost inflatable and drop-in structures that last long enough to prevent severe damage—and effective means for re-routing flood water.

Hurricane Katrina also dramatically underscored the grave potential for devastation when levees fail. One challenge that must be overcome is the fact that most of the levees were not built or are not maintained by the U.S. Army Corps of Engineers; most are in state, local or private ownership—some 40,000 miles within the Los Angeles coastal region, alone. IGD has thus put in place several **Levee Strengthening andDamage Mitigation Projects** to protect low-lying areas from floods that over-top or destroy levees; the program has three primary thrusts: (1) develop levee-screening tools and methodologies to detect potential failures; (2) enhance levee-protection by using innovative techniques to prevent levee failure; and (3) demonstrate the feasibility of one or more rapidly deployable systems for stopping the flow of water through a breach within six hours of its formation. The division is working with engineers in the United States and overseas, especially The Netherlands, with its hundreds of years of experience in levees, dikes and dams. We will continue efforts to demonstrate rapid response and recovery technologies, leading to transition of "best-of-breed" solutions by FY 2012.

The **Preparedness and Response Advanced Concepts, Technologies and Systems Programs** are developing advanced technologies, tools and equipment to support rapid and effective all-hazards emergency response and recovery; it addresses, as well, advanced technologies to improve the ability of first responders to instantly track, locate and identify responders in challenged areas (e.g., subterranean facilities, skyscrapers and warehouses). In FY 2008, the **Personal Protective Equipment Project** is developing materials that can provide CBRNE protection to first responders. Important protective properties include: self-decontamination for chemical and/or biological agents, increased service life, self-healing upon compromise (e.g., ripped) and flame resistance. Special studies have developed the system requirements and designs for a first responder three-dimensional location system for tracking personnel, and prototype hardware and software for a structural-integrity monitoring system to assess the stability of structures prior to entry.

FIVE ::
A FUTURE OF HOPE & SECURITY

The people, processes, plans and programs are in place to deliver cost-effective, innovative, perhaps revolutionary but certainly timely science and technology solutions for America's homeland security—today and for as long as necessary—against terrorism and natural or man-made disasters.

The DHS S&T Directorate is the proponent of America's technological asymmetric advantage against a broad spectrum of threats, hazards and challenges to the nation's safety and security. Our dedicated scientists, engineers, thinkers and support people—and our partners in government, industry and academia world wide—will continue to push the boundaries of imagination and challenge, committed to ensuring that new mission-critical capabilities are created, knowledge is generated, a world-class STEM workforce is enhanced, and effective, reliable and affordable technologies are deployed to the right people, at the right places and at the right times.

We shall not fail or falter;
we shall not weaken or tire.
Neither the shock of battle
nor the long-drawn trials of
vigilance and exertion will wear
us down. Give us the tools and
we will finish the job.

Winston Churchill
1941

"In the realm of ideas, everything depends on enthusiasm," Goethe recognized, but "in the real world, all rests on perseverance." Perseverance and enthusiasm are and will remain the hallmarks of the men and women who are the heart of our Homeland Security S&T Enterprise. We will not want for imagination or initiative or agility as we work to ensure a safer nation and world.

FOR THE TRANSPORTATION SECURITY ADMINISTRATION

- **Home Made Explosives** signature data that informed the decision to allow air travelers to carry small quantities of liquids
- **Screening Passenger by Observation Techniques** analysis that delivers enhanced capabilities in detecting suspicious behavior through cross-culturally validated observational and interview techniques that can be employed well before a person commits a hostile act
- **Behavior-Based Deception-Detection Training** enables cross-cultural validation of behavioral indicators of deception and suspicious behavior
- **Hand-Held Vapor-Detection** technology to detect and identify persistent but low-vapor pressure chemical threats on surfaces

FOR OTHER U.S. GOVERNMENT AGENCIES

- The **National Bioforensics Analysis Center** that conducts forensic analysis of evidence from biocrime or bioterrorism events
- High-throughput **integrated mobile laboratories** for broad-based tactical chemical analysis
- Material threat determinations to inform Health and Human Service's medical countermeasure requirements generation
- End-to-end **BioTerrorism Risk Assessment, Chemical Terrorism Risk Assessment** and integrated **CBRNE Risk Assessment** capabilities to assess cross-threat risks and evaluate risk-mitigation strategies
- The **Biodefense Knowledge Center** that provides tailored, in-depth biodefense analysis and "24/7" operational support
- The **Chemical Security Analysis Center** that analyses current and evolving chemical threats and provides "24/7" technical reach-back support
- The **Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks** tool that provides automated analysis of possible attack paths through a cyber network for attack correlation, prediction and response
- A **secure USB device** that corrects a significant cyber-security vulnerability

FOR STATE AND LOCAL FIRST-RESPONDERS

- A man-portable **Interoperable Tactical Operations Center**
- The **critical infrastructure inspection** management system that enables officers to locate quickly and inspect critical infrastructure
- Seven **hurricane scenario models** for New York City restoration planning
- Guidance for **critical transportation facilities** following a biological incident
- A networked **chemical detection system** for rail transportation facilities
- A nationwide **validation and testing program for communications equipment** to ensure interoperability

FOR EVERY ONE

- A **Global Terrorism Database** containing more than 85,000 events to analyze and understand factors that influence the likelihood of a terrorist attack

www.dhs.gov
March 2008