High-Priority Technology Needs

May 2009

Homeland Security

Science and Technology

Version 3.0

U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

Science and Technology

May 2009

Delivery of homeland security technological capabilities is what the DHS S&T Directorate is all about. We *know* what our customers need, and you'll find an overview of those needs in this booklet. We *don't know* where the good ideas will come from. That's why we're offering this-third edition booklet to you. Share it with your colleagues. You can also find it on the Web at www.dhs.gov.

We are delighted to speak with you anytime, anywhere, if you believe you can bring us a technology that meets a customer requirement.

Since the last edition, we've added requirements from our newly commissioned 13th Integrated Product Team devoted to state, local, tribal, and territorial first responders and emergency managers.

I hope you find this useful. Thanks for all you do to help keep the Nation safer.

Bradley I. Buswell
Under Secretary (Acting)
Science and Technology Directorate
U.S. Department of Homeland Security

The S&T Capstone Transition Program

DHS S&T's Transition Program is customer-focused and output-oriented. The Directorate's near-term efforts are aligned to our DHS customers' critical needs in the form of Enabling Homeland Capabilities (EHCs), consisting of technologies that can be developed, matured, delivered, and commercialized or validated as a standard within a 3-year period.

A formalized, structured process, the DHS Transition Program aligns investments to Agency requirements and is managed by Capstone Integrated Product Teams (IPTs). These teams consist of our DHS customers and critical stakeholders and are specifically chartered to ensure that technologies are engineered and integrated into systems scheduled for delivery and made available to DHS customers. Investments are competitively selected and focus on DHS's highest-priority requirements that provide capability to DHS operating components and first responders.

With the addition of the First Responder Capstone IPT, there are now 13 Capstone IPTs in the following functional areas:

1. First Responder
2. Border Security
3. Cargo Security
4. Maritime Security
5. Cyber Security
6. Information Sharing
7. Interoperability
8. Transportation Security
9. Counter-IED
10. Chemical/Biological Defense
11. People Screening
12. Infrastructure Protection
13. Incident Management

The DHS S&T Transition Program is continuously evolving through incorporation of best practices from industry and other federal partners. As priorities change, the process is flexible enough to accommodate necessary changes while maintaining the stability of prior-year decisions.

Please note that each Capstone IPT page has block text and italic text. The block text denotes information that was presented in the previous version of this booklet. Italic text denotes new/revised information.

DHS S&T's Six Technical Divisions

The mission of the Department of Homeland Security is to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that may occur. The strategies the Science & Technology Directorate will use to accomplish those Department goals and make the Nation safer are:

The S&T Directorate's **Explosives Division** promotes the development of effective techniques to protect our citizens and our country's infrastructure against the devastating effects of explosives by seeking innovative approaches in detection and in countermeasures. It provides the concepts, science, technologies, and systems that increase protection from explosives and promotes the development of field equipment, technologies, and procedures to interdict suicide bombers, car and truck bombs, and shoulder-fired missiles before they can reach their targets.

The S&T **Chemical/Biological Division** seeks out the science needed to reduce the probability and potential consequences of a biological pathogen or a chemical attack on the Nation's civilian population, its infrastructure, or its agricultural system. The division develops and implements early detection and warning systems for attack characterization. Priorities include research and development efforts on urban monitoring, detection technologies, bioassays, a bioforensics capability, and restoration and response tools and technologies.

When making critical decisions—from evacuating civilians from a hurricane's path to preventing a terrorist attack—responders and planners need information that is relevant, accurate, and timely. S&T's **Command, Control and Interoperability Division** (CID) provides the technologies, processes, infrastructure, and mechanisms that allow these decision-makers to gather, analyze, manage, protect, and share critically needed homeland-security information, be it voice, data, or imagery.

The mission of the **Borders and Maritime Security Division** is to develop and transition technical capabilities that enhance U.S. border security without impeding commerce & travelers' flow. The Division serves as the Nation's primary shepherd of Cargo, Borders and Maritime Security science and technology with areas of responsibility that encompass all air, land and maritime borders (including U.S. ports-of-entry and inland waterways). BMD understands the technical dimension of homeland security challenges and provides customers with new and/or better options to accomplish their mission.

S&T looks at biometrics, motivation and intent, hostile intent, human factors engineering, and the social/behavioral/economic sciences to improve detection, analysis, and understanding of threats posed by individuals, groups, and radical movements. The efforts of the S&T **Human Factors/Behavioral Sciences Division** support the preparedness, response, and recovery of communities affected by catastrophic events.

The need to protect the country's 18 areas of critical infrastructure from acts of terrorism, natural disasters, and accident, is paramount, but so are state and local preparedness and response. S&T's **Infrastructure/Geophysical Division** addresses physical, cyber, and human elements of our Nation's vulnerable infrastructure, focusing on capabilities, needs, and gaps, and on known threats.

In short, when dedicated scientists, engineers, and thinkers push the boundaries of challenge, and when they are committed to the security of our Nation, they can help ensure that new mission-critical capabilities are created, knowledge is generated, and needed technologies are deployed to the right places.

DHS Customers and Customers of Our Customers

DHS S&T enables its customers—the DHS components—and their customers on the front lines, with technical capabilities to carry out their missions. Customers include state, local, and tribal entities, Border Patrol agents, Coast Guardsmen, Customs officials, Federal Air Marshals, airport baggage screeners, and first responders at the state, local, tribal and territorial levels. The responders—fire fighters, police, emergency medical technicians, and bomb disposal experts—act decisively to protect people and property, to tend to the injured, and to bring a measure of calm and clear thinking to chaotic situations. DHS S&T supports them with the tools they need to perform their jobs more efficiently, quickly, and safely, and with greater accuracy.

S&T customers, like USCG and CBP, oversee 95,000 miles of coastline, lakes, and inland waterways and 7,500 miles of the U.S. border. They safeguard 327 official ports of entry—by air, land and sea. Other customers protect the critical infrastructure that keeps our society functioning—the hospitals and public health facilities, schools, transportation systems, water supply, power plants, food supply—and the cyber backbone that underpins essential services—and much more.

Through processes like our Capstone Integrated Product Teams, S&T works with our customers in defining the capabilities they need to secure the Nation. We bring key stakeholders in the process to the table to establish a plan for getting needed capabilities into the development or acquisition pipeline so that vital needs are addressed.

Homeland Security

U.S. Citizenship and Immigration Services

U.S. Customs and Border Protection

U.S. Immigration and Customs Enforcement

Transportation Security Administration

FEMA

Support to Front Line > 23 Million

- Port Security
- Public Health
- Hospitals
- Transportation
- Emergency Management
- Clinics
- Venue Security
- Public Works/Utility
- School Security
- Response Volunteers

FIRST RESPONDER

DHS Lead: FEMA; Office of Intelligence and Analysis (OI&A); National Protection and Programs Directorate (NPPD)

The First Responder Capstone IPT coordinates the identification and prioritization of technology requirements and capability gaps of the Federal, state, local, territorial and tribal first responders. Identified technology solutions will be designed, tested, and assessed for usability and commercialized for the first responder community.

REPRESENTATIVE TECHNOLOGY NEEDS

- Capability to interrogate a vehicle at range and perform diagnostic and defeat procedures on explosives (Explosives Division/C-IED Capstone IPT)
- Non-lethal compliance measures for people, vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel (Borders and Maritime Security Division/Border Security Capstone IPT)
- Personnel-safe, handheld non-intrusive inspection devices that allow for the inspection of hidden or closed compartments (Borders and Maritime Security Division/Border Security Capstone IPT)
- Capability for law-enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials. Improved screening and examination by non-intrusive inspection (Borders and Maritime Security Division/Cargo Security Capstone IPT)
- Capability to enhance disaster preparedness in communities (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Respiratory protection against airborne particulate matter and poisonous gases—in particular, protective breathing equipment during the clean-up and recovery process (Chemical/Biological Division and Infrastructure and Geophysical Division/Chemical-Biological Defense Capstone IPT and Incident Management Capstone IPT)
- Capability to predict criminal and terrorist activity (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Cost-effective training technologies for first responders depicting real-world scenarios (Infrastructure and Geophysical Division/Incident Management Capstone IPT)
- Enhanced ambulance safety and improved ambulance situational awareness and voice/data communications (Command, Control and Interoperability Division/Interoperability Capstone IPT)
- Enhanced capability to identify individuals and verify the professional credentials of individuals in both pre-planned and developing events (Human Factors/Behavioral Sciences/People Screening Capstone IPT)
- Provide emergency managers with seamless data, voice, and video information for enhanced situational awareness in major and minor crisis (Command, Control and Interoperability Division/Interoperability Capstone IPT)
- Enhanced information management capabilities to make available information more useful. In particular, the enhanced integration and intelligent prioritization of information (Command, Control and Interoperability Division/Interoperability Capstone IPT)

Randel Zeller, Director of Interagency and First Responder Programs
Email: IAD-FirstResponder@dhs.gov

BORDER SECURITY

DHS Leads: Customs and Border Protection and Immigration and Customs Enforcement

Border security represents a myriad of challenges. Detection and identification, and, when required, apprehension and law enforcement, represent a significant portion of the DHS mission. The Border Security IPT works to prioritize functional mission needs and to identify solution space for the path to successful technology development. This leads to the development of mature technologies that support rapid, coordinated, and safe responses to anomalies and threats against the Nation and the personnel assigned to conduct the mission. The primary Federal customers for the IPT are U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), who represent end users such as Border Patrol agents, CBP Air and Marine personnel, and ICE special agents.

REPRESENTATIVE TECHNOLOGY NEEDS

- Detection, tracking, and classifying of all threats along the terrestrial and maritime border—in particular, technologies to support tunnel detection and rugged terrain, concealing foliage, water obstacles, mountains, and other environmental constraints (Borders and Maritime Security Division)
- Personnel-safe, handheld, non-intrusive inspection device that allow the inspection of hidden or closed compartments—*in particular, the ability to find contraband and security threats (people) through steel walls. Unit must contain sensor and active source, if required, in same device. Technologies other than x-ray, gamma rays, and neutrons are desired.* (Borders and Maritime Security Division)
- Ability for law enforcement officers to assure compliance of lawful orders using non-lethal means—in particular, the ability to disable vehicles/vessels and temporarily incapacitate persons to prevent the infliction of damage or harm (Borders and Maritime Security Division)
- Improved analysis and decision-making tools that will ensure the development and implementation of border security initiatives—*in particular, a decision support effort researching automated evaluation of proposed actions through expert systems and modeling and simulation for border security. The effort is researching ways to fully integrate multiple domains, including technology, managerial, policy, organizational, political, and contextual, to enhance decision making* (Borders and Maritime Security Division)
- Non-lethal compliance measures for vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel—*in particular, the use of a compact, tuned, and focused energy system to shut down or disrupt normal vehicle operation while leaving the breaking and steering unaffected* (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security
Email: SandT-BordersMaritime@dhs.gov

CARGO SECURITY

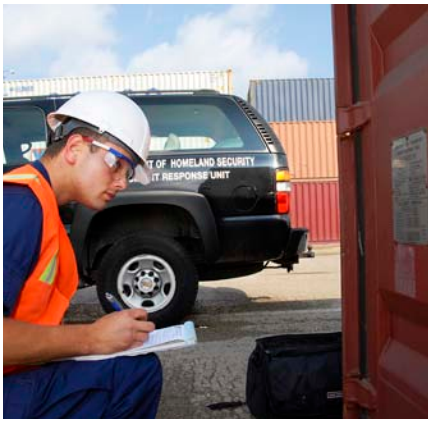
DHS Lead: Customs and Border Protection

The Cargo Security IPT provides guidance for the development of technology and the accumulation of knowledge that address the difficult issues associated with managing the Nation's supply chain of incoming and outgoing goods and commodities. This IPT focuses on the operational needs of U.S. Customs and Border Protection (CBP) and the Transportation Security Administration (TSA), with DHS Policy and the U.S. Coast Guard as high-level stakeholders. The user community associated with the technologies and knowledge products developed in this IPT area consists of CBP Office of Field Operations (OFO) Officers, TSA Officers, and the private-sector shipping companies. The Cargo Security IPT is concerned with the full spectrum of requirements associated with improved and reliable scanning of cargo and conveyances for unauthorized items and personnel, associated information management, intrusion detection, and other anomalies while maintaining the steady flow of commerce. The IPT takes a system-of-systems, integrated approach toward development of technological solutions that will satisfy clearly stated mission requirements.

REPRESENTATIVE TECHNOLOGY NEEDS

- Improved screening and examination by non-intrusive inspection—in particular, the ability to detect or identify contraband items (for example, drugs, money, illegal firearms), threat materials, or stowaways; improve penetration, resolution, throughput, contrast sensitivity, reliability, mobility, and interoperability; and integrate with future Automated Target Recognition capability (Borders and Maritime Security Division)
- Increased information fusion, anomaly detection, Automatic Target Recognition—in particular, automated imagery detection capability for anomalous content (e.g., stowaways, hidden compartments, contraband), and the ability to detect anomalous patterns in shipping data (Borders and Maritime Security Division)
- Capability to screen 100 percent of air cargo—*in particular, the use of next generation non-intrusive inspection systems to detect and identify contraband items or stowaways without disrupting the flow of commerce* (Borders and Maritime Security Division)
- Track domestic high-threat cargo—in particular, the ability to track DHS-designated Toxic Inhalation Hazardous (TIH) cargos in domestic transit (Borders and Maritime Security Division)
- Positively identify cargo and detect intrusion or unauthorized access—in particular, in containerized, palletized, parcel, or bulk/break-bulk maritime and air cargo (Borders and Maritime Security Division)
- Reliable container seal security/detect intrusion devices—*in particular, combining six-sided container/conveyance intrusion detection with the ability to sense the presence of harmful or hazardous materials (e.g., explosives, RADNUC, Chemical, and Biological agents)* (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security
Email: SandT-BordersMaritime@dhs.gov



MARITIME SECURITY

DHS Lead: United States Coast Guard

The U.S. maritime environment is a great expanse, requiring several DHS operational components to properly manage and monitor its boundaries. The Maritime Security Capstone IPT is responsible for gathering and prioritizing the requirements from a variety of members and stakeholders, including: U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), U.S. Immigrations and Customs Enforcement (ICE), and Transportation Security Administration (TSA). The IPT is focused on improving communication, sensors, and surveillance capabilities for its customer components, leading to better operational situation awareness and management of mission-related information. Deliverables resulting from the deliberations of the Maritime Security IPT will feed and enable DHS policy, cross-component acquisition and procurement decisions through technology development and/or knowledge building.

REPRESENTATIVE TECHNOLOGY NEEDS

- Wide-area surveillance from the coast to beyond the horizon, including port and inland waterways, for detection, ID, & tracking— In particular, the detection of vessels between the port region and beyond the horizon, especially small vessels with the capability to geo-reference the images (Borders and Maritime Security Division)
- Improve the capability to continuously track contraband on ships or containers—in particular the ability to conceal transponders while maintaining effective transmissions (Borders and Maritime Security Division)
- Vessel compliance through less-lethal compliance methods—*in particular, exploring a variety of technical approaches to interdict illegal migrant operations, contraband transport, fishing, security threats, or general law violations* (Borders and Maritime Security Division)
- Ability for law enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials—*in particular, a safe, lightweight, non-intrusive inspection device for chemicals, explosives, and drugs featuring one-step operation and able to identify multiple threats (chemical warfare agents, toxic industrial chemicals, explosive chemicals, drugs) with one unit/one setup, operating on portable power, wearable, self-contained, using non-contact methodology to sample suspected contraband items* (Borders and Maritime Security Division)
- Improved radar performance for detection and tracking of large and small vessels in the port and coastal regions—*in particular, through the use of more advanced signal processing* (Borders and Maritime Security Division)

Anh Duong, Division Head, Borders and Maritime Security
Email: SandT-BordersMaritime@dhs.gov

CYBER SECURITY

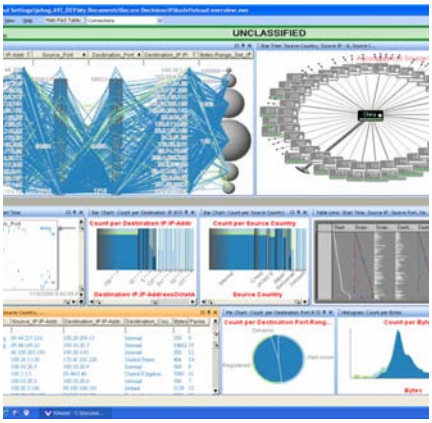
DHS Lead: National Cyber Security Center, United States Secret Service, National Protection and Programs Directorate

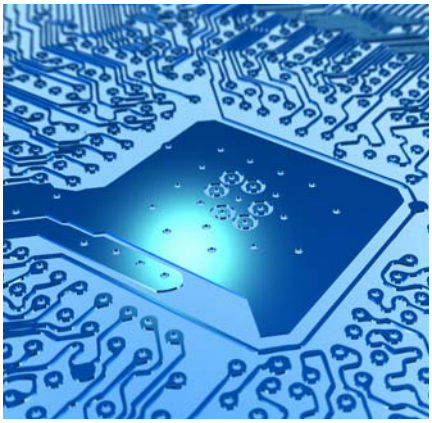
The Cyber Security Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The program conducts research, development, testing, evaluation, and transition activities focused on protecting critical information infrastructure; developing the cyber research infrastructure; and delivering new technologies to relevant end users.

REPRESENTATIVE TECHNOLOGY NEEDS

- Secure Internet protocols, including standard security methods (Command, Control and Interoperability Division)
- Improved capability to model the effects of cyber attacks—in particular, measuring security and risk in IT infrastructure components and understanding of Internet topography (Command, Control and Interoperability Division)
- Software Testing and Vulnerability Analysis Technologies—*in particular, services and capabilities to rigorously and routinely build, test, and analyze source and binary forms of software in realistic conditions representative of operational environments* (Command, Control and Interoperability Division)
- Usable Security—*in particular, focused technologies that demonstrate new ways to address the confluence of usability and security* (Command, Control and Interoperability Division)
- Information-system insider-threat detection models and mitigation technologies—in particular, technology aids that increase the accuracy, reduce the time, and reduce the cost of detecting and discovering unauthorized insiders (Command, Control and Interoperability Division)
- Analytical techniques for security across the IT system-engineering lifecycle—in particular, analytical techniques to facilitate detecting, quantifying, measuring, visualizing, and understanding system security (Command, Control and Interoperability Division)
- Process Control Systems (PCS) security—in particular capabilities for metrics, wireless communications, and system vulnerability assessment. (Command, Control and Interoperability Division)
- Cyber Forensics—*in particular, cyber-related tools and investigative techniques that support law enforcement to address the full range of investigating and solving cyber related crimes* (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, and Interoperability
Email: SandT-C2I@dhs.gov





INFORMATION SHARING

DHS Lead: Office of Intelligence & Analysis

The Information Sharing Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The current information-sharing environment consists of communities that have developed their own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. The Information Sharing program is developing national solutions for sharing all-hazards information in a manner consistent with national security and legal standards that create new technologies to share, search, and analyze homeland security information across jurisdictional boundaries; provide technologies to enable a distributed, secure, and trusted environment for transforming data into actionable information; and recognize and leverage the vital roles played by state and major urban area information fusion centers.

REPRESENTATIVE TECHNOLOGY NEEDS

- Data fusion from law enforcement, intelligence partners, and other sensors to support a user-defined operating picture (UDOP)—in particular, technologies to correlate and fuse sensor data into a comprehensive representation (Command, Control and Interoperability Division)
- Management of user identities, rights, and authorities—In particular, technologies and standards to enable external identity adjudication (Command, Control and Interoperability Division—shared between Information Sharing and Cyber Security)
- Distribution of intelligence products—in particular, technologies and techniques to automate the distribution of unclassified or lower classification portions of intelligence information to DHS mission partners (Command, Control and Interoperability Division)
- Information sharing within and across sectors on terrorist threats—in particular, analytic capabilities for structured, unstructured, and streaming data (Command, Control and Interoperability Division)
- Improvement of situational awareness and decision support horizontally across Federal Law Enforcement and Intelligence partners as well as vertically through Federal, state, local and tribal partners —*in particular, technologies that provide automated, dynamic, real-time data processing and visualization capability and the information sharing protocols that enable them* (Command, Control and Interoperability Division)
- Predictive analytics—in particular, the ability to correlate data and information for recognizing and potentially predicting terrorist attack patterns (Command, Control and Interoperability Division)
- Protection of U.S. citizen personal data—in particular, advanced data integrity techniques to automatically purge or anonymize personally identifiable information (Command, Control and Interoperability Division)
- Improved cross-agency reporting of suspicious activity—in particular, technologies that would improve real-time awareness through alerting others to and sharing information about suspicious activities and persons (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, and Interoperability
Email: SandT-C2I@dhs.gov

INTEROPERABILITY

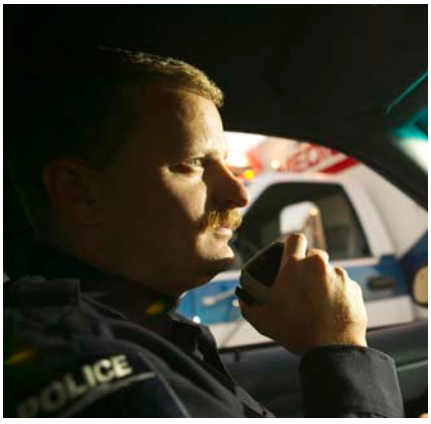
DHS Leads: Federal Emergency Management Agency and Office of Emergency Communications

Relevant and timely information is vital for making tactical, strategic, and planning decisions when responding to natural and man-made incidents and disasters. The Interoperability Capstone IPT provides homeland security practitioners with a toolkit of technologies, processes, and mechanisms to support gathering, analyzing, managing, sharing, and protecting information. The Interoperability program primarily supports the "sharing" aspect by developing solutions related to land mobile radio communications; interoperable voice and data applications; public-safety-grade communications networks; and public alert and warning systems.

REPRESENTATIVE TECHNOLOGY NEEDS

- Accelerate the development of voluntary consensus standards for interoperable communications, including Project 25 and Voice over Internet Protocol. (Command, Control and Interoperability Division)
- Standardize, pilot, and evaluate wireless broadband technologies and applications across multiple networks. (Command, Control and Interoperability Division)
- Develop message interface standards and architectures that enable emergency-information sharing, data exchange, and public alerts and notifications. (Command, Control and Interoperability Division)
- Perform interoperable communications standards compliance testing on emergency response devices and systems. (Command, Control and Interoperability Division)
- Test and evaluate multi-band radio technologies for use in emergency communications and day-to-day operations. (Command, Control and Interoperability Division)
- Develop standards, applications, and technologies to enable seamless access to voice, data, and imagery via a single, unified communications device. (Command, Control and Interoperability Division)
- Develop ad-hoc and mesh networks to link local, state, and Federal personnel in emergency situations and other security events. (Command, Control and Interoperability Division)

Dave Boyd, Division Head, Command, Control, & Interoperability
Email: SandT-C2I@dhs.gov



TRANSPORTATION SECURITY

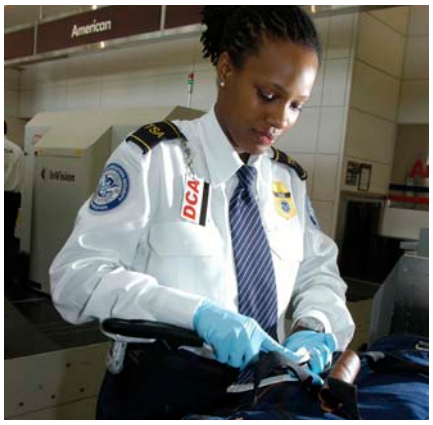
DHS Lead: Transportation Security Administration

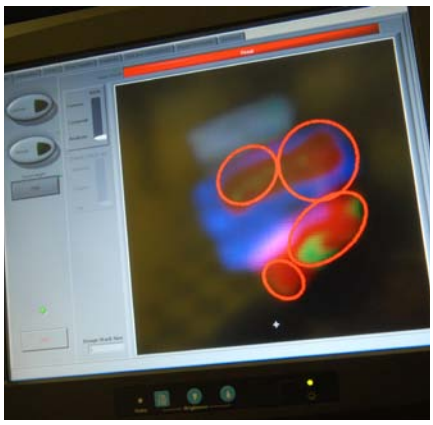
Hundreds of thousands of people and tons of cargo move across the nation every day by air, rail, highway, and mass transit systems. The Transportation Security Capstone IPT is pursuing technology solutions that make all modes of transportation safe while still enabling the freedom of movement for people and commerce. Because there is no one technology solution, the IPT takes a layered systems approach to create a strong, formidable system that protects against current and emerging threats.

REPRESENTATIVE TECHNOLOGY NEEDS

- The capability to screen people for explosives and weapons at fixed checkpoints—in particular, technologies that allow higher detection rates with minimal disruption to passenger flow (Explosives Division)
- The capability to detect homemade explosives (HME)—*in particular, characterization of HME threats and damage effects and development of HME detection technologies* (Explosives Division)
- Automated systems solution for explosives and weapons detection in checked and carried baggage—*in particular, automated systems to screen for conventional and homemade explosives and weapons* (Explosives Division)
- Optimization of canine explosive detection capability—*in particular, non-hazardous, low-cost canine training aids* (Explosives Division)
- The capability to screen air cargo for explosives and explosive devices—in particular, technologies for screening break-bulk and palletized air cargo (Explosives Division)

Jim Tuttle, Division Head, Explosives
Email: SandT-Explosives@dhs.gov





COUNTER-IED

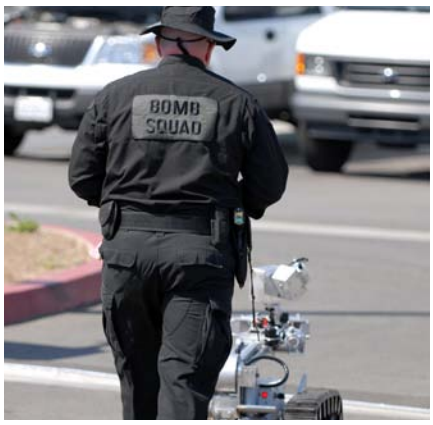
DHS Leads: Office of Bombing Prevention and United States Secret Service

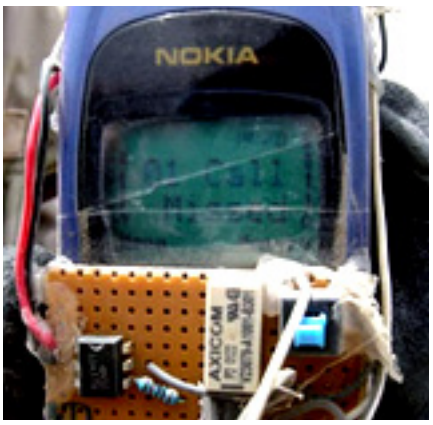
There is no single technology solution to counter the threat of an attack by an improvised explosive device (IED). For this reason, the C-IED Capstone IPT has taken a layered systems approach and is developing technology solutions that can be injected at each stage in the IED attack timeline. (Other emerging counter-IED technology solutions are also being developed in S&T's basic research portfolio).

REPRESENTATIVE TECHNOLOGY NEEDS

- *Capability to identify and model the human precursors of IED threats and terrorist activity within CONUS using unstructured data and novel computational models* (Human Factors/Behavioral Sciences Division)
- Capability to *predict participants and locations of potential IED attacks* based on existing or known geospatial, socio-cultural, and behavioral information (Human Factors/Behavioral Sciences Division)
- Capability to non-intrusively detect vehicle-borne IEDs—in particular, technologies to detect the explosive or explosive device (Explosives Division)
- Capability to detect person-borne IEDs from a standoff distance—in particular, technologies to detect the explosive or explosive device (Explosives Division)
- Capability to defeat vehicle-borne IEDs—in particular, non-explosive and standoff defeat technologies (Explosives Division)
- Capability to defeat person-borne and leave-behind IEDs (Explosives Division)
- Capability to diagnose vehicle-borne and person-borne IEDs (Explosives Division)
- Capability to diagnose and defeat water-borne IEDs, above and below the waterline (Explosives Division)
- Capability to characterize IED threats, including IED design, assembly, detonation, and effects (Explosives Division)

Jim Tuttle, Division Head, Explosives
Email: SandT-Explosives@dhs.gov





CHEMICAL/BIOLOGICAL DEFENSE

DHS Leads: Office of Infrastructure Protection and Office of Health Affairs

The Chemical/Biological Defense Capstone IPT improves the understanding, technologies, and systems needed to anticipate, deter, protect against, detect, mitigate, and recover from biological and chemical attacks on the Nation's population, agriculture, and infrastructure. The program's mission is "to work to increase the Nation's preparedness against chemical and biological threats through improved threat awareness, advanced surveillance and detection, and protective countermeasures."

REPRESENTATIVE TECHNOLOGY NEEDS

- Improved chemical-biological forensic analysis capability (Chemical/Biological Division)
- Handheld rapid biological and chemical detection systems—in particular, technology that distinguishes between threat and non-threat agents and technology to assist with detection and deterrence while the normal stream of commerce continues (Chemical/Biological Division)
- Detection paradigms and systems for improved, emerging, and novel biological threats (Chemical/Biological Division)
- Tools to detect and mitigate animal disease outbreaks (Chemical/Biological Division)
- Analytic tools for accessing and integrating diverse data from multiple domains to enhance biological surveillance (Chemical/Biological Division)
- National-scale detection architectures and strategies to address outdoor and indoor environments (for example, highly trafficked transportation hubs) and critical infrastructure (Chemical/Biological Division)
- Tools to enable assessment of potential consequences of attacks on chemical facilities and chemical–biological attacks on other critical infrastructure (Chemical/Biological Division)
- Integrated CBRNE sensor reporting capability—in particular, the integration of sensors into a common operating picture for easy integration of future detection systems (Chemical/Biological Division)
- New techniques for analysis of chemical threat agent samples, chemical warfare agents, toxic industrial materials and nontraditional agents to develop chemical signatures that supplement traditional forensic techniques. (Chemical/Biological Division)
- Improved tools for integrated CBRN risk assessment (Chemical/Biological Division)
- Incident characterization capability for response and restoration—in particular, fully integrated operational tools to support surveillance, detection, incident characterization, and response systems; plus, a systems approach to characterize the extent of contamination and the restoration of wide urban areas, including high-traffic areas (transit/transportation facilities) following a chemical or biological agent release (Chemical/Biological Division)
- *Integrated system for chemical and biological agent detection in buildings* (Chemical/Biological Division)
- Mechanisms to independently evaluate and validate commercially developed assays for the first-responder community (Chemical/Biological Division)
- *Improved methods of decontamination of biological and chemical contamination from both fixed (e.g., buildings) and moving (e.g., vehicles) infrastructure* (Chemical/Biological Division)
- *Rapid means of interrogation and inspection of closed packages and cargo for illicit chemical and biological threat materials* (Chemical/Biological Division)

Beth George, Division Head, Chemical/Biological
Email: SandT-ChemBio@dhs.gov

PEOPLE SCREENING

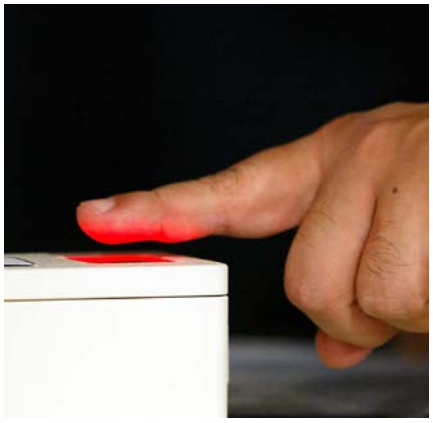
DHS Leads: Screening Coordination Office and Citizenship & Immigration Services

The people Screening Capstone IPT advances national security by developing and applying the social, behavioral, and physical sciences to provide rapid, accurate, non-invasive, user-friendly and publicly acceptable capabilities to improve identification and analysis of unknown and known threats posed by individuals, groups, and radical movements.

REPRESENTATIVE TECHNOLOGY NEEDS

- Systematic collection and analysis of information related to understanding a terrorist group's intent to engage in violence—in particular, data fusion and modeling and simulation capability to provide a near-real-time assessment (Human Factors/Behavioral Sciences Division)
- Real-time detection of deception or hostile intent—in particular, the development of non-invasive behavioral sensors *and analytical methods* (Human Factors/Behavioral Sciences Division)
- Capability *to acquire biometrics in challenging operational environments and provide* real-time positive verification of an individual's identity, using multiple biometrics—*in particular, face, fingerprint, and iris biometrics* (Human Factors/Behavioral Sciences Division)
- Mobile biometrics screening capabilities, including handheld, ten-fingerprint-capture, *face and iris*, environmentally hardened, wireless, and secure devices (Human Factors/Behavioral Sciences Division)
- High-speed, high-fidelity, ten-print capture capability (Human Factors/Behavioral Sciences Division)
- Rapid, *cost-effective* DNA testing to verify family relationships during interviews for the disposition of benefits (*under $100 per test; ultimately within 45 minutes for testing*) (Human Factors/Behavioral Sciences Division)
- Remote, standoff biometric detection for identifying individuals at a distance (Human Factors/Behavioral Sciences Division)
- *Maximize screener performance at checkpoints through selection and training, and through the use of advanced imaging technologies.* (Human Factors/Behavioral Sciences Division)

Sharla Rausch, Division Head, Human Factors/Behavioral Sciences
Email: SandT-HumanFactors@dhs.gov



INFRASTRUCTURE PROTECTION

DHS Lead: Office of Infrastructure Protection

The Infrastructure Protection Capstone IPT mission is to improve the Nation's preparedness for, and response to, natural and man-made threats to critical infrastructure. The IPT develops technical solutions and reach-back capabilities to improve Federal, state, local, tribal, and private-sector preparedness and response efforts to all-hazards events that impact the Nation's critical infrastructure. The primary Federal customers for the IPT are the Department of Homeland Security's (DHS's) Office of Infrastructure Protection (IP), the National Protection and Programs Directorate (NPPD), and critical infrastructure owners and operators.

REPRESENTATIVE TECHNOLOGY NEEDS

- High-Resolution Analytical tools to accurately quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors—*in particular, tools for natural and man-made disruptions* (Infrastructure and Geophysical Division)
- Effective and affordable blast analysis and protection for critical infrastructure; improved understanding of blast failure mechanisms and protection measures for the most vital assets through the development of suites of advanced materials, design procedures, and innovative construction methods to protect CI/KR (Infrastructure and Geophysical Division)
- Advanced, automated and affordable monitoring and surveillance—in particular, decision support systems, and mitigation strategies to prevent disruption and build in resiliency (Infrastructure and Geophysical Division)
- Rapid mitigation and recovery technologies to quickly reduce the effect of natural and man-made disruptions and cascading effects (Infrastructure and Geophysical Division)
- Critical utility components that are affordable, highly transportable, and provide robust solutions during man-made and natural disruptions (Infrastructure and Geophysical Division)
- *Systems to provide early warning capabilities for early detection and notice of potential levee failures* (Infrastructure and Geophysical Division)

Chris Doyle, Division Head, Infrastructure and Geophysical
Email: SandT-InfrastructureGeophysical@dhs.gov

INCIDENT MANAGEMENT

DHS Leads: Federal Emergency Management Agency and Office of Emergency Communications

The Incident Management Capstone IPT mission is to improve the Nation's preparedness for, and response to, natural and man-made threats through superior situational awareness and emergency response capabilities. The IPT develops technical solutions and reach-back capabilities to improve Federal, state, local, tribal, and private-sector preparedness and response efforts to all-hazards events that impact the United States' people and economy. The primary Federal customer for the IPT is the Federal Emergency Management Agency (FEMA), which represents end users, including first responders and Federal, state, and local emergency managers.

REPRESENTATIVE TECHNOLOGY NEEDS

- Integrated modeling, mapping, and simulation capability—in particular, an integrated and simulation-based incident planning and response capability to analyze all-hazard disaster response and recovery operations, tactics, techniques, plans, and procedures for use in a real-time environment for simulation-based training (Infrastructure and Geophysical Division)
- Personnel monitoring (emergency responder 3-D locator system) capability—*in particular, X/Y/Z accuracy of better than 1 meter in a multilevel building providing incident commanders the ability to rapidly track and effectively deply or redeploy first responders in a challenging environment* (Infrastructure and Geophysical Division)
- Personnel monitoring (physiological monitoring of firefighters) capability—*in particular, an integrated body-worn sensor suite to provide real-time health analysis and issue alarms to both wearer and command staff, reducing risk of responder cardio/cerebral fatalities through early identification and mitigation* (Infrastructure and Geophysical Division)
- Incident management enterprise system—in particular, increased situational awareness to manage available and anticipated human and material resources, transportation capabilities, and the need for timely information to support critical decisions involving rapidly shifting priorities; geospatial data to create a seamless system between Federal, state, and local first responders; and established virtual continuity of operations (COOP) capabilities to improve incident management when key infrastructures and facilities are unavailable (Infrastructure and Geophysical Division)
- Logistics management tool—*in particular, technologies to effectively manage critical resources and provide complete resource situational awareness at all levels of government, down to point of consumption, and return* (Infrastructure and Geophysical Division)

Chris Doyle, Division Head, Infrastructure and Geophysical
Email: SandT-InfrastructureGeophysical@dhs.gov

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. **http://www.hsarpabaa.com**

- **Small Business Innovation Research (SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. **http://www.sbir.dhs.gov**

- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. **https://www.safetyact.gov/**

- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, state, local, and tribal first responders by fielding prototypical solutions within 12 months at a cost less than $1 million per project. **www.dhs.gov/techsolutions**

- **The Long Range BAA** identifies strategic topics of interest to DHS's mission and is the a principal vehicle for white papers and full proposals. Submissions are assessed based on the stated evaluation criteria and the overall best value to the government. **https://baa.st.dhs.gov/**



Commercialization Office

The U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate's commercialization efforts are headed by the Commercialization Office, which was officially established in October 2008. The mission of the Commercialization Office is to develop and execute programs and processes that identify, evaluate, and commercialize widely distributed products or services that meet the detailed operational requirements of DHS's operating components, the first responder community, critical infrastructure/key resources (CI/KR) owners and operators, and other Department users. Managing and enhancing DHS S&T's outreach effort with the private sector to establish and foster mutually beneficial working relationships leading to the fielding of technologies to secure the Nation is a primary day-to-day function of the Commercialization Office.

The SECURE Program—one of the Commercialization Office's innovative public–private partnerships enables the rapid, cost-effective and efficient development of products and services to protect the Homeland to the benefit of the taxpayers, the private sector, and DHS. The goal of the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) program is to leverage the resources of the private sector to develop solutions aligned with (and tested against) DHS-generated and vetted detailed operational requirements, using the private sector's experience and resources. DHS stakeholders can then make better-informed decisions on products or services specifically aligned to their requirements. (See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

COMMERCIALIZATION OFFICE RESOURCES

In order to facilitate outreach to the private sector and improve communications, the Commercialization Office has published a number of materials, including briefs, books, and articles that outline the major activities of the Commercialization Office and provide readers with easy-to-understand guides for requirements developed and the recently developed and implemented DHS commercialization process. The Commercialization Office also reaches out to businesses of all kinds—disadvantaged, small, medium and large—about opportunities that exist for partnership. The Commercialization Office makes these resources available to all who are interested. Please visit our Web site at http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm.

Requirements Development Resources: The Commercialization Office has published three popular books to assist in the development of detailed operational requirements [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)]. These books serve as useful resources to explain the critical role of detailed requirements in the cost-effective and efficient development of products and services.

Commercialization Office Articles: The Commercialization Office has published more than 25 articles and a compilation of works ["Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good" (February 2009)] written at the request of the private sector to inform the public of new opportunities and ways to work with DHS. The articles inform readers about processes and the benefits of fostering a mutually beneficial partnership with DHS. Article topics include the critical role of requirements, focus the role of small and disadvantaged businesses, global outreach efforts and potential available markets.

Other Resources: In addition, the Commercialization Office has made available a number of presentations, a program concepts-of-operations, and a product realization chart that correlates terminology used by both the public and private sector to delineate how science, technology development, and product development are related to basic research, innovation, and transition, using a Technology Readiness Level (TRL) "backbone."

Feedback Welcomed! For more information on how to get involved in programs like SECURE or to provide feedback to the Commercialization Office, please send an e-mail to sandt_commercialization@hq.dhs.gov.

Frequently Asked Questions

1. Who submits a technology need for consideration?

DHS solicits requirements inputs from all communities that carry out Homeland Security missions, such as DHS Components (Coast Guard, ICE, CBP, ICE, TSA, Secret Service, and FEMA etc), end users, first responders, and state, local, and tribal authorities.

2. What is the benefit from working with DHS S&T?

Working with DHS S&T can provide business opportunities to:

- Provide technical services and expertise that address important National Security needs.
- Develop and manufacture widely distributed products for end users.
- Better understand DHS current and future needs to effectively respond to DHS solicitations.

3. Is DHS S&T interested in assessing existing products that appear to meet or address a technology need identified here?

YES. If you believe you have a product that meets or addresses a need stated in this booklet, email the division point of contact (POC) for the Capstone IPT relevant to your field. State which need your product addresses and briefly provide any supporting material that describes your product and how it specifically addresses that need. Your email will be directed to a Subject Matter Expert (SME) within the division for evaluation and assessment. You will be notified of the division's interested in pursuing further discussions with you regarding your product.

4. What is the best way to determine DHS S&T interest in a research idea?

First contact the S&T POC whose division best matches the research field of interest. This person will attempt to match up the research or technology development with the correct person(s) within the S&T Directorate. Those contemplating submission of a white paper or full proposal may obtain valuable insight about whether their expertise and interest is a good match for research currently being funded by S&T.

If interest is indicated, The Long Range BAA is a principal vehicle for submitting white papers and full proposals. It is recommended that a white paper be the first step before expending the time and expense of submitting a full proposal. Submissions are assessed based on the stated evaluation criteria and overall best value to the government. Multiple contract awards can be made based upon the proposal's evaluation, funding availability and priorities, and other programmatic considerations. Awards may take the form of contracts, grants, cooperative agreements, or other transaction (OTAs) agreements, as appropriate.

DHS S&T Points of Contact:

- **Starnes Walker**
  Director of Research
  Email: SandT-Research@dhs.gov

- **Roger McGinnis**
  Director of Innovation
  Email: SandT-Innovation@dhs.gov

- **Rich Kikla**
  Director of Transition
  Email: SandT-Transition@dhs.gov

- **Randel Zeller**
  Director of Interagency and First Responder Programs
  Email: IAD-FirstResponder@dhs.gov

- **Jim Tuttle**
  Division Head, Explosives
  Email: SandT-Explosives@dhs.gov

- **Beth George**
  Division Head, Chemical/Biological
  Email: SandT-ChemBio@dhs.gov

- **Dave Boyd**
  Division Head, Command, Control, and Interoperability
  Email: SandT-C2I@dhs.gov

- **Anh Duong**
  Division Head, Borders and Maritime Security
  Email: SandT-BordersMaritime@dhs.gov

- **Sharla Rausch**
  Division Head, Human Factors/Behavioral Sciences
  Email: SandT-HumanFactors@dhs.gov

- **Chris Doyle**
  Division Head, Infrastructure and Geophysical
  Email: SandT-InfrastructureGeophysical@dhs.gov

From Science and Technology...
Security and Trust