High-Priority Technology Needs

June 2008

Homeland Security

Science and Technology

Version 2.0

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

Homeland Security

Science and Technology

June 2008

Science and Technology Directorate investments are tied directly to technology gaps identified by my customers. Those customers are represented by the senior leadership of the agencies and components that comprise DHS. These leaders of DHS work continuously with specialists, technologists, and program managers, as well as acquisition professionals, to ensure that investments meet their objectives, and if successful, can be procured. I also have a responsibility to invest in technological breakthroughs for the "customers of my customers" – the national heroes who are the first responders of America. DHS S&T is continuing to develop the means for greater first responder participation in the definition of capability gaps in order to ensure their high priority needs are met.

This booklet summarizes technology areas identified for further work by all these customers. I've included contact information for my key leadership. I hope you find this booklet useful.

Jay M Cohen

The Hon. Jay M. Cohen
Under Secretary
Science and Technology Directorate
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.

Capstone IPTs have been established for twelve Homeland Security functional areas:

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

The DHS S&T Transition Program is a continuously evolving program that incorporates best practices from industry and allows continual process improvement. As priorities change, the process is flexible enough to accommodate any necessary redirection 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 **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.

The attack on 9/11 demonstrated profoundly the danger to first responders and the public when those responding to emergencies cannot communicate effectively. The ability to talk across disciplines and jurisdictions systems, exchanging voice and/or data on demand, in real time, when authorized, is critically important, as is having disaster management plans to deal with crises. The S&T Directorate's **Command, Control, and Interoperability Division** addresses the intricately related issues of reliable day-to-day public safety communications, as well as the security of our cyber world.

The S&T **Borders and Maritime Security Division** focuses on preventing the entry of illegals and terrorists while ensuring an efficient flow of lawful commerce, visitors, and citizens. It looks at technologies to protect and strengthen our ports of entry, technologies that can prescreen all high-risk entities coming into the country, and entry/exit tracking capabilities. It also looks at new technologies for detecting, identifying, and classifying high-interest vessels, and capabilities for wide-area monitoring of maritime traffic.

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 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 also 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.

Border Security

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

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 & Maritime Security Division)
- Improved ballistic protection via personal protective equipment—*In particular, a focus on increased effectiveness against a wider-range projectile type, plus lighter weight and integrated helmet protection* (Borders & Maritime Security Division)
- Non-destructive tools that allow the inspection of hidden or closed compartments—*In particular, the ability to find contraband and security threats* (Borders & 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 & Maritime Security Division)
- Ability for law enforcement personnel to quickly identify the origin of gunfire and classify the type of weapon fired (Borders & Maritime Security Division)
- Improved analysis and decision-making tools that will ensure the development and implementation of border security initiatives (Borders & Maritime Security Division)
- Non-lethal compliance measures for vehicles, vessels, or aircraft, allowing safe interdiction by law enforcement personnel (Borders & Maritime Security Division)

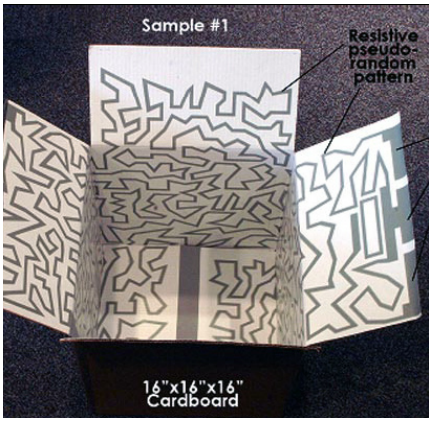
BORDER SECURITY

Cargo Security

DHS Lead: Customs & Border Protection

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 & Maritime Security Division)
- Increased information fusion, anomaly detection, Automatic Target Recognition capability—*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 & Maritime Security Division)
- Detect and identify WMD materials and contraband—*In particular, the ability to detect chemical and biological threats, explosives, and contraband* (Borders & Maritime Security Division)
- Capability to screen 100 percent of air cargo (Borders & 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 & Maritime Security Division)
- Positively ID cargo and detect intrusion or unauthorized access—*In particular, in containerized, palletized, parcel, or bulk/break-bulk maritime and air cargo* (Borders & Maritime Security Division)
- Reliable container seal security/detect intrusion devices (Borders & Maritime Security Division)



Chem/Bio Defense

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

Representative Technology Needs

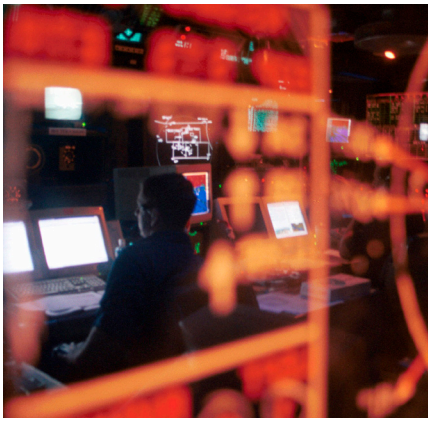
- Improved Chem-Bio Forensic Analysis capability (Chemical & Biological Division)
- Handheld rapid biological and chemical detection systems—*In particular, technology that distinguishes between threat and non-threat agents. Technology to assist with detection and deterrence while the normal stream of commerce continues* (Chemical & Biological Division)
- Policy net assessments to provide fresh perspectives on fundamental elements of the national biodefense strategy—*In particular, support to HSPD-10 pillars: Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery* (Chemical & Biological Division)
- Detection paradigms and systems for improved, emerging, and novel biological threats (Chemical & Biological Division)
- Tools to detect and mitigate animal disease breakouts (Chemical & Biological Division)
- National-scale detection architectures and strategies to address outdoor and indoor (for example, highly trafficked transportation hubs) and critical infrastructure (Chemical & Biological Division)
- Consequence assessment of attacks on chemical facilities and Chem-Bio 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)
- 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)
- *Mechanisms to independently evaluate and validate commercially developed assays for the first-responder community to be public health actionable* (Chemical & Biological Division)
- *Tools for sampling, rapidly detecting, and identifying in the field illegal products, including high-consequence pathogens and toxins that threaten agriculture and the food industry* (Chemical & Biological Division)

Cyber Security

DHS Lead: Cyber Security & Communications

Representative Technology Needs

- Secure Internet protocols, including standard security methods (Command, Control, & 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, & Interoperability Division)
- Comprehensive next-generation network models—*In particular, models that apply to the design, construction, and evaluation of IT systems to improve cyber security and information* (Command, Control, & Interoperability Division)
- Composable and scalable secure systems—*In particular, technology and long-term research to develop more robust transitional systems and security architectures* (Command, Control, & Interoperability Division)
- Technologies and standards for managing the identities, rights, and authorities used in an organization's networks (Command, Control, & 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, & 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, & Interoperability Division)
- Process Control Systems (PCS) security—*In particular, capabilities for metrics, wireless communications, and system vulnerability assessment* (Command, Control, & Interoperability Division)



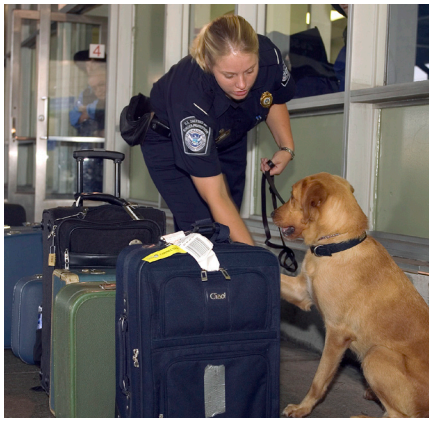
The DHS Science and Technology Capstone Integrated Product Team (IPT) process is a dynamic effort responsi
threat of improvised explosive devices, DHS re-aligned the Explosives Capstone IPT into two Capstone IPTs focu
mass transit, and maritime), checkpoint screening (people and materials), checked item screening (includes
(IED) Capstone IPT will develop technologies to predict, detect, defeat, mitigate, and respond to explosive atta

Transportation Security

DHS Lead: Transportation Security Administration

Representative Technology Needs

- Technologies to screen people for explosives and weapons at fixed aviation and mass-transit checkpoints—*In particular, to allow higher detection rates with minimal disruption to passenger flow* (Explosives Division)
- System solutions for explosives detection in checked and carried bags—*In particular, automated systems to screen for conventional explosives, liquids, weapons, and homemade explosives* (Explosives Division)
- Capability to detect homemade or novel explosives—*In particular, characterizing potential homemade explosives for use in developing detection systems for screening at checkpoints* (Explosives Division)
- Optimized canine explosive detection capability—*In particular, techniques, training tools, and methods to improve performance for all transportation venues* (Explosives Division)
- Technologies for screening air cargo for explosives and explosive devices—*In particular, technologies for screening break-bulk, palletized, and containerized air cargo* (Explosives Division)

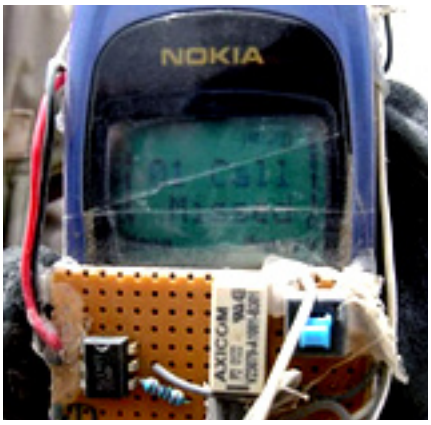


ve to the ever changing threat to our nation. In recognition of the importance of transportation security and the used on these threats. The Transportation Security Capstone IPT will address security for venue areas (airports, Air Cargo), explosives characterization, and homemade explosives. The Counter-Improvised Explosive Device cks.

Counter IED

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

Representative Technology Needs



- Capability to detect domestic use vehicle-borne improvised explosive devices (VBIEDs)—*In particular, technologies to provide a non-intrusive means of screening vehicles for VBIED detection* (Explosives Division)
- Capability to assess, render safe, and neutralize explosive threats—*In particular, technologies to protect against person- and vehicle-borne explosive threats* (Explosives Division)
- *Capability to detect person-borne IEDs from a standoff distance—In particular, technology to enable the detection of person-borne concealed explosive threats in various high-throughput venues, at standoff distances* (Explosives Division)
- *Capability of inerting common explosives or making them less sensitive to initiation* (Explosives Division)
- *Techniques to track the origin of explosives and bomb components used in domestic IEDs—In particular, to improve forensic evidence investigations with better tools such as biometric technology, taggants, and radio-frequency identification devices (RFIDs)* (Explosives Division)
- *Capability to mark explosives material to improve the detection of IEDs* (Explosives Division)
- *Low-cost and practical approaches to protect urban structures and occupants from VBIED attacks* (Infrastructure & Geophysical Division)
- *Protective measures to reduce damage and prevent catastrophic failure of high-consequence infrastructure assets subjected to IED attacks* (Infrastructure & Geophysical Division)
- *Models for predicting of blast effects that take into account the diversity and variability of construction in urban settings* (Infrastructure & Geophysical Division)
- *Affordable blast-, fragment-, and fire-resistant materials* (Infrastructure & Geophysical Division)
- *Rapidly deployable blast-mitigation concepts for rapid threat response or temporary protection* (Infrastructure & Geophysical Division)
- *Tools to rapidly assess damaged structures* (Infrastructure & Geophysical Division)
- *Techniques and tools to stabilize damaged structures and prevent their collapse* (Infrastructure & Geophysical Division)
- *Capability to predict the threat of an IED attack* (Human Factors Division)
- *Increased capability at vehicle or pedestrian ports of entry and border crossings to identify person born IED threats* (Human Factors Division)
- *Enhanced capability for local officials to communicate understandable and credible IED warnings and instructions to the public* (Human Factors Division)

Incident Management

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

Representative Technology Needs

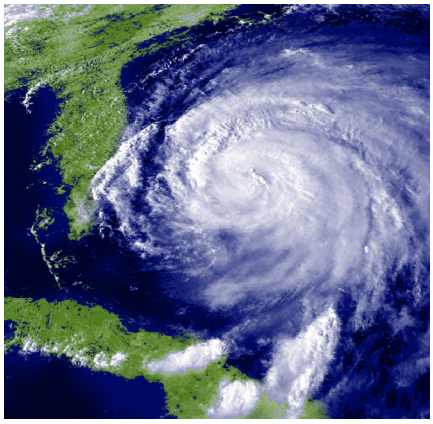
- Integrated modeling, mapping, and simulation capability—*In particular, an integrated and simulation-based incident planning and response capability to analyze all-hazard disaster response and recovery operations, tactics, techniques, plans, and procedures for use in a real-time environment for simulation-based training* (Infrastructure & Geophysical Division)

- Personnel monitoring (emergency responder 3-D locator system) capability—*In particular, X/Y/Z accuracy of better than 1 meter in multi-level buildings and challenging environments* (Infrastructure & Geophysical Division)

- Personnel monitoring (physiological monitoring of firefighters) capability—*In particular, integrated body-worn sensor suite to provide real-time health analysis and issue alarms to both wearer and command staff* (Infrastructure & 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 & Geophysical Division)

- Logistics management tool—*In particular, technologies to effectively manage critical resources and provide improved situational awareness at all levels of government* (Infrastructure & Geophysical Division)



Information Sharing

DHS Lead: Office of Intelligence & Analysis

Representative Technology Needs

- Data fusion from law enforcement, intelligence partners, and other sensors to support the common operating picture (COP)—*In particular, technologies to correlate and fuse sensor data into a comprehensive representation* (Command, Control, & Interoperability Division)
- Management of user identities, rights, and authorities—*In particular, technologies and standards to enable external identity adjudication* (Command, Control, & Interoperability Division)
- 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, & Interoperability Division)
- Information sharing within and across sectors on terrorist threats—*In particular, analytic capabilities for structured, unstructured, and streaming data* (Command, Control, & Interoperability Division)
- Improvement of situational awareness and decision support—*In particular, technologies that provide automated, dynamic, real-time data processing and visualization capability* (Command, Control, & Interoperability Division)
- Situational awareness between U.S. Coast Guard and partners—*In particular, maritime and law enforcement information-sharing protocols* (Command, Control, & Interoperability Division)
- *Predictive analytics—In particular, the ability to correlate data and information for recognizing and potentially predicting terrorist attack patterns* (Command, Control, & 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, & 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, & Interoperability Division)

Infrastructure Protection

DHS Lead: Office of Infrastructure Protection

Representative Technology Needs

- Analytical tools to quantify interdependencies and cascading consequences as disruptions occur across critical infrastructure sectors—*In particular, tools for natural and manmade disruptions* (Infrastructure & Geophysical Division)
- Effective and affordable blast analysis and protection for critical infrastructure, and an improved understanding of blast-failure mechanisms and protection measures for the most vital critical infrastructures and key resources (CI/KR) (Infrastructure & Geophysical Division)
- Advanced, automated, and affordable monitoring and surveillance technologies—*In particular, decision support systems to prevent disruption, mitigate results, and build in resiliency* (Infrastructure & Geophysical Division)
- *Rapid mitigation and recovery technologies to quickly reduce the effect of natural and manmade disruptions and cascading effects* (Infrastructure & Geophysical Division)
- *Critical utility components that are affordable, highly transportable, and provide robust solutions during manmade and natural disruptions* (Infrastructure & Geophysical Division)

Interoperability

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

Representative Technology Needs

- Accelerate the development of Project 25 and Internet Protocol (IP) interfaces (Command, Control, & Interoperability Division)
- Standardize, pilot, and evaluate emergent wireless broadband data technologies and applications (Command, Control, & Interoperability Division)
- Develop message interface standards that enable emergency-information sharing and data exchange—*In particular, develop eXtensible Markup Language (XML) standards for communications software, systems, and devices* (Command, Control, & Interoperability Division)
- Develop complementary test procedures—*In particular, testing and evaluation of multi-band radios for civilian use in emergency communications and day-to-day operations* (Command, Control, & Interoperability Division)
- *Provide seamless access to voice and data networks, using a unified communications device—In particular, identify and refine potential platforms, interfaces, and applications* (Command, Control, & Interoperability Division)
- *Perform interoperability compliance testing on emergency response communications devices and systems—In particular, develop and execute an interoperability compliance assessment program* (Command, Control, & Interoperability Division)

MARITIME SECURITY

Maritime Security

DHS Lead: United States Coast Guard

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 & Maritime Security Division)

- Data fusion and automated tools for command center operations—*In particular, the ability to view entire scenes and provide alerts about anomalous and illegal activity; the automation of the ability to compare current tasking and location of blue forces to new events and recommend courses of action; and the improved ability for agencies to share information and collaborate when not colocated* (Borders & 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 & Maritime Security Division)

- Develop improved ballistic personal protective equipment for officer safety (Borders & Maritime Security Division)

- Vessel compliance through less-lethal compliance methods (Borders & Maritime Security Division)

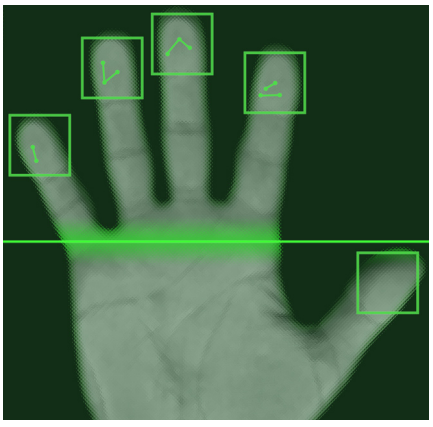
- *Ability for law-enforcement personnel to detect and identify narcotics, chemical warfare agents, toxic industrial chemicals, explosives, and contraband materials—In particular, the ability to identify multiple threats with one unit/one setup; operate on portable power; be wearable and self contained; and be able to sample for and detect contraband without direct contact* (Borders & Maritime Security Division)

People Screening

DHS Leads: Screening Coordination Office and Citizenship & Immigration Services

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 Division)
- Real-time detection of deception or hostile intent—*In particular, the development of non-invasive behavioral sensors* (Human Factors Division)
- Capability in real time for positive verification of an individual's identity, using multiple biometrics—*In particular, face, fingerprint, and iris biometrics* (Human Factors Division)
- Capability for secure, non-contact electronic credentials; contactless readers or remote interrogation technologies for electronic credentials (Human Factors Division)
- Mobile biometrics screening capabilities, including handheld, *ten-fingerprint-capture, environmentally hardened,* wireless, and secure devices (Human Factors Division)
- High-speed, high-fidelity ten-print capture capability (Human Factors Division)
- *Rapid DNA testing to verify family relationships during interviews for the disposition of benefits* (Human Factors Division)
- *Remote, standoff biometrics detection for identifying individuals at a distance* (Human Factors Division)



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 $1M per project. **www.dhs.gov/techsolutions**

- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reaches out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at **S&T-Commercialization@dhs.gov**.

DHS S&T Points of Contact:

- **Starnes Walker**
  Director of Research
  Email: S&T-Research@dhs.gov

- **Roger McGinnis**
  Director of Innovation
  Email: S&T-Innovation@dhs.gov

- **Rich Kikla**
  Director of Transition (Acting)
  Email: S&T-Transition@dhs.gov

- **Jim Tuttle**
  Division Head, Explosives
  Email: S&T-Explosives@dhs.gov

- **Elizabeth George**
  Division Head, Chemical & Biological
  Email: S&T-ChemBio@dhs.gov

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

- **Dave Newton**
  Division Head (Acting), Borders & Maritime Security
  Email: S&T-BordersMaritime@dhs.gov

- **Sharla Rausch**
  Division Head, Human Factors
  Email: S&T-HumanFactors@dhs.gov

- **Chris Doyle**
  Division Head, Infrastructure & Geophysical
  Email: S&T-InfrastructureGeophysical@dhs.gov

From Science and Technology...
Security and Trust