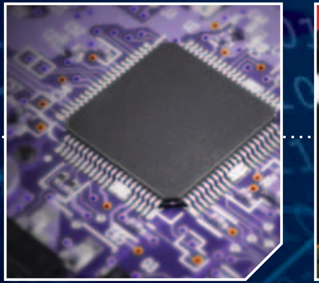
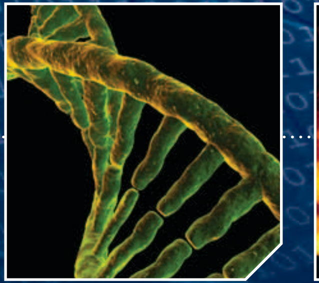




Strategic Plan 2015–2019

Science and Technology Directorate

Homeland
Security

Science and Technology

MESSAGE FROM THE UNDER SECRETARY

The Science and Technology Directorate's (S&T) mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise. The successful execution of this mission rests significantly on whether we can transform our approach to research and development (R&D). This plan serves as the directorate's roadmap for how it plans to serve as a model for federal R&D.

In crafting this plan, I made four observations that I think are important to keep in mind as we implement this plan and pursue this goal. First, the Department of Homeland Security's operational and oversight responsibilities are enormous. As a department, we face complex operational threats and provide a range of solutions from tactical niche solutions to vast national-level capabilities. Second, I believe a balanced R&D portfolio teeming with innovative and force multiplying solutions is critical to ensuring the safety, security, and resilience of the homeland. Providing frontline operators with tools that secure them the upper hand in their respective environments is paramount. Third, S&T has a passionate and dedicated workforce. Walking the halls, I am invigorated by the widespread enthusiasm for our mission. Our workforce is hungry to contribute, and we have the technical expertise and depth to work hand-in-hand with operators and end users. Fourth, the federal government is no longer the majority provider of R&D funding, and we can no longer assume we have access to the best minds if we work exclusively through who and what we already know. To be a 21st-century R&D organization, we must tap innovation engines in the venture capital world, Silicon Valley, and universities. The more vehicles there are to work with those performers, the more effectively and efficiently S&T can develop security solutions.

To turn these observations into action we will look to this Strategic Plan and our five Visionary Goals—Screening At Speed, a Trusted Cyber Future, Enable the Decision Maker, Responder of the Future, and Resilient Communities—to guide our resource investments and unite our staff. These goals serve as our "North Star" and the basis for S&T's strategy. Equally important is how we deliver on these goals. We will choose projects strategically, ensuring they are force multipliers that address critical end-user needs and are aligned with the investments of our partner R&D organizations and industry. We will focus on energizing the Homeland Security Industrial Base to invest in future capabilities that will ensure the safety, security, and resilience of our nation. Finally, we will establish a strong and healthy leadership culture within the directorate.

I fully endorse the implementation of the *S&T Strategic Plan 2015–2019.*

Dr. Reginald Brothers
Under Secretary for Science and Technology
Department of Homeland Security

TABLE OF CONTENTS

EXECUTIVE SUMMARY

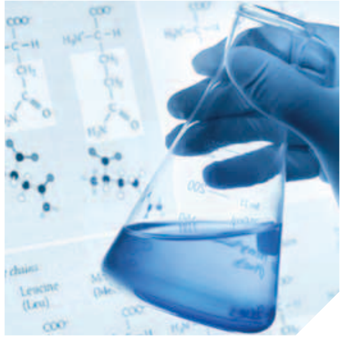
The Science and Technology Directorate (S&T) plays a critical role in addressing major homeland security threats for the Department of Homeland Security (DHS). S&T uses the knowledge of science and tools of technology to make our country, our communities, and our families more secure across the broad spectrum of threats facing the homeland—from counterterrorism to natural disasters. As the research and development (R&D) arm of DHS, S&T is responsible for leading R&D, demonstration, testing, and evaluation activities to ensure a safer, more secure nation.

S&T developed the *S&T Strategic Plan 2015–2019* to outline strategic objectives, initiatives, and activities for the next five years. Through the implementation of this plan and investment in a balanced portfolio of work, S&T will position the department to address the challenges of both today and tomorrow. Part I of this plan introduces the directorate and characterizes the strategic context it operates within. Part II of this strategic plan details the specific objectives, initiatives, and activities S&T will conduct in the next five years. Finally, Part III of this plan details S&T's R&D Capability Roadmaps, which will guide investments in the years to come.

PART I – Introduction and Strategic Context

S&T is one of a handful of DHS components created from whole cloth under the Homeland Security Act of 2002. In the last 12 years, the directorate has grown into a trusted partner for DHS operators and state, local, tribal, and territorial first responders. It is important to recognize that although R&D is the backbone of this organization, S&T maintains a diverse and complex set of roles and responsibilities that extend beyond a traditional R&D organization. These roles and responsibilities enable the directorate to serve as the glue between operational elements.

This strategic plan serves as the directorate's roadmap for how it will become a model for federal R&D. The plan's three strategic objectives were specifically designed to address the environment the directorate operates within today. Additionally, pursuant to guidance outlined in Secretary of Homeland Security Jeh Johnson's "Strengthening Departmental Unity of Effort" memo, the directorate established Visionary Goals. These goals will serve as 30-year horizon points to drive innovation within S&T and its ecosystem of technical expertise inside and outside of government.



EXECUTIVE SUMMARY CONTINUED

PART II – The Strategy

To keep pace with evolving threats and security challenges, S&T will implement several strategic objectives and initiatives. Through this work, S&T will ensure DHS is poised to bridge current capability gaps as well as anticipate homeland security challenges 20 to 30 years ahead.

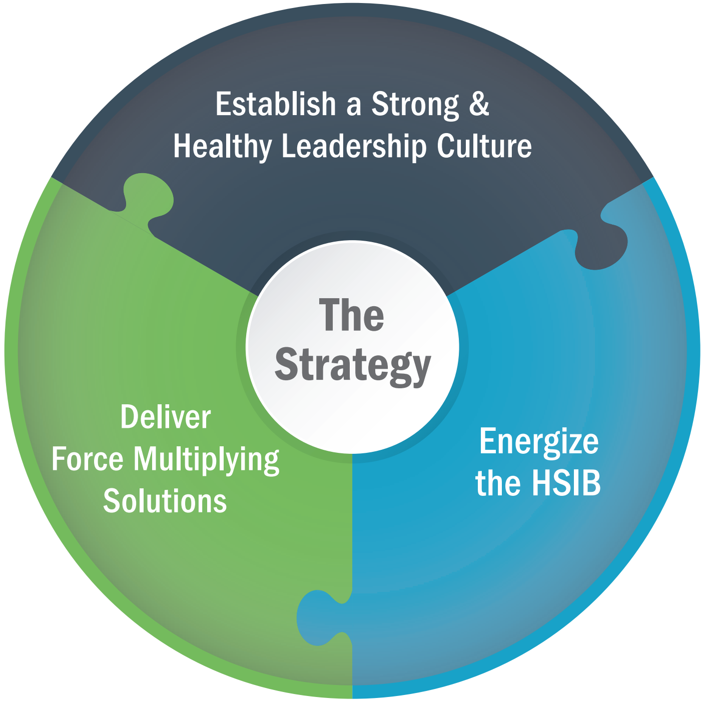
The strategic plan details specific activities S&T will lead to achieve the objectives and initiatives laid out here:

Deliver Force Multiplying Solutions: S&T must focus its limited resources on delivering force multiplying solutions designed to address the highest priority needs. S&T's framework to achieve this objective involves the following interdependent initiatives:

Identify and Prioritize Operational Requirements and Capability Gaps – S&T actively participates in departmental and interagency governance bodies, as well as activities that enable direct engagement with operators, to identify and prioritize operational requirements and capability gaps.

Make Strategic Investments in High-impact, Priority Areas – The directorate's ability to make strategic investments in high-impact, priority areas is dependent upon the cultivation of a balanced R&D portfolio and continued investment in national and directorate capabilities that enable R&D.

Partner with the Homeland Security Enterprise (HSE) – S&T must continuously invest in the creation and maintenance of partnerships with DHS components and other R&D organizations. Internal and external partnerships are a core element of our strategy and serve as the foundation of S&T's innovative ecosystem.


Establish a Strong & Healthy Leadership Culture
The Strategy
Deliver Force Multiplying Solutions
Energize the HSIB

Energize the Homeland Security Industrial Base (HSIB): S&T will employ a robust array of tools to enhance private sector outreach, technology awareness, and R&D contracting. To achieve this objective, S&T will execute the following initiatives:

Optimize Markets by Pooling Demand and Developing Standards – S&T is working to integrate markets with international partners and to develop standards jointly with industry to better coordinate R&D investments, pool demand, and reduce costs.

EXECUTIVE SUMMARY CONTINUED

Engage the HSIB through a Deliberate, Continuous, and Transparent Approach – S&T will facilitate regular idea exchange between operational users and industry-based technologists by deploying new, non-traditional outreach mechanisms.

Improve Programs Designed to Increase Collaboration with Innovative Companies – S&T will develop new approaches to engage non-traditional companies and revamp existing programs to become more timely and dynamic. Additionally, S&T will reengineer internal forecasting capabilities to better understand where to capitalize on industry investment trends.

Establish a Strong and Healthy Leadership Culture: S&T's ability to achieve the aforementioned strategic objectives depends upon common identity, clarity of mission, and leadership at all levels of the organization. With empowerment, responsibility, and accountability as cultural values, S&T strives both to create an innovation-friendly environment and to give staff the tools and opportunities to grow and succeed within it. The following initiatives will enable S&T to fulfill this objective:

Empower the Workforce – S&T will give a stronger voice to staff and foster a broader sense of ownership and attachment to the organization and its direction. S&T values our workforce's perspective and believes that none of us individually is as smart as all of us collectively.

Provide Meaningful Leadership Development and Professional Growth Opportunities – Diffusing leadership throughout S&T gives staff more input in and power over the direction of the organization. To make this possible, S&T will make targeted investments in tools and capabilities that ensure our workforce has the skills, competencies, and knowledge required to advance S&T's mission at all levels. S&T will further enable our staff by providing substantive training and workforce development opportunities.

Engineer a Pipeline for the Next Generation of Homeland Security Professionals – To ensure that its future workforce sustains and builds on successes, S&T is committed to growing a pipeline for the next generation of staff. This two-part activity involves a continuous assessment of the organization that includes analyzing where staff needs will grow or decline and making long-term investments in growing areas to ensure that emerging workforce needs are addressed.

PART III – S&T Research and Development Strategic Priorities

Each of S&T's five Homeland Security Advanced Research Projects Agency divisions, three First Responders Group divisions, and Apex programs and Technology Engines have developed Capability Roadmaps aligned to the needs of their operational end users. These high-level roadmaps formalize a vision, identify strategic drivers, provide future capability descriptions, and list R&D objectives for the next five years. In collaboration with HSE end users and HSIB partners, S&T's investment in projects aligned to these roadmaps will prepare the department for the challenges of both today and tomorrow.

INTRODUCTION AND STRATEGIC CONTEXT

Part I

INTRODUCTION AND STRATEGIC CONTEXT

The Science and Technology Directorate (S&T) is one of a handful of components in the Department of Homeland Security (DHS) created from whole cloth under the Homeland Security Act of 2002. In the last 12 years, the directorate has grown into a trusted partner for DHS operators and state, local, tribal, and territorial first responders. It is important to recognize that, although research and development (R&D) is the backbone of this organization, S&T maintains a diverse and complex set of roles and responsibilities that extend beyond a traditional R&D organization. These nontraditional R&D organization roles and responsibilities include, but are not limited to: (a) the coordination and administration of operational test and evaluation for all major DHS acquisitions; (b) the implementation of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002; (c) in collaboration with the Office of the General Counsel, the management of the department's intellectual property portfolio; (d) in collaboration with all elements of DHS, the maintenance of the department's compliance with treaties such as the Biological Weapons Convention; and (e) the operation and maintenance of enduring national capabilities such as laboratories. These roles and responsibilities enable the directorate to serve as the glue between operational elements.

Through considerable work and dedication from its workforce, S&T has made the most of an industrial-age toolbox in a digital-age R&D landscape. This strategic plan serves as the directorate's roadmap for how it plans to serve as a model for federal R&D—hyper-connected, capable of meeting increasing demand for return on taxpayer dollars, and tailored to the digital age. The plan's three strategic objectives were specifically designed to address the strategic context of the environment the directorate operates within today.

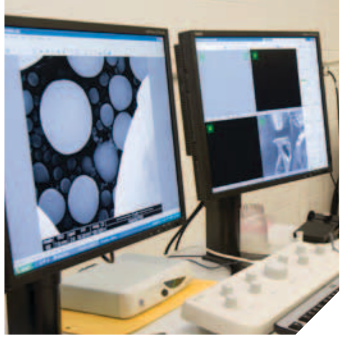
Given the current and projected threat environments, technology and R&D are the bridge to the future of homeland security. The most effective and efficient changes will come with the smart application of science and technical expertise to develop force multiplying solutions. These technology-based solutions will provide homeland security operators and first responders the upper hand in their respective operational spaces. They will also enable the Homeland Security Enterprise (HSE) to expand capabilities and security coverage, despite limited funds. Thus, the directorate's strategic objective to deliver force multiplying solutions is critical in the department's ability to fulfill its mission and operational demands.

HOMELAND SECURITY ENTERPRISE

Homeland security is a widely distributed and diverse national enterprise. The term enterprise refers to the collective efforts and shared responsibilities of those involved in maintaining critical homeland security capabilities. S&T considers the HSE and our international partners as our constituency—those we work with and for—to enhance our nation's security and resiliency.

DHS Components and Staff	**First Responders**
Federal Partnerships/the Interagency	**International Community**
Industry	**Academia**
Private Citizens	**Critical Infrastructure Owners and Operators**

S&T and the Homeland Security Industrial Base (HSIB) serve an enterprise that has a diverse set of needs, operates in a resource-constrained budget environment, conducts procurements in a sometimes fragmented way, and is often criticized for transparency and

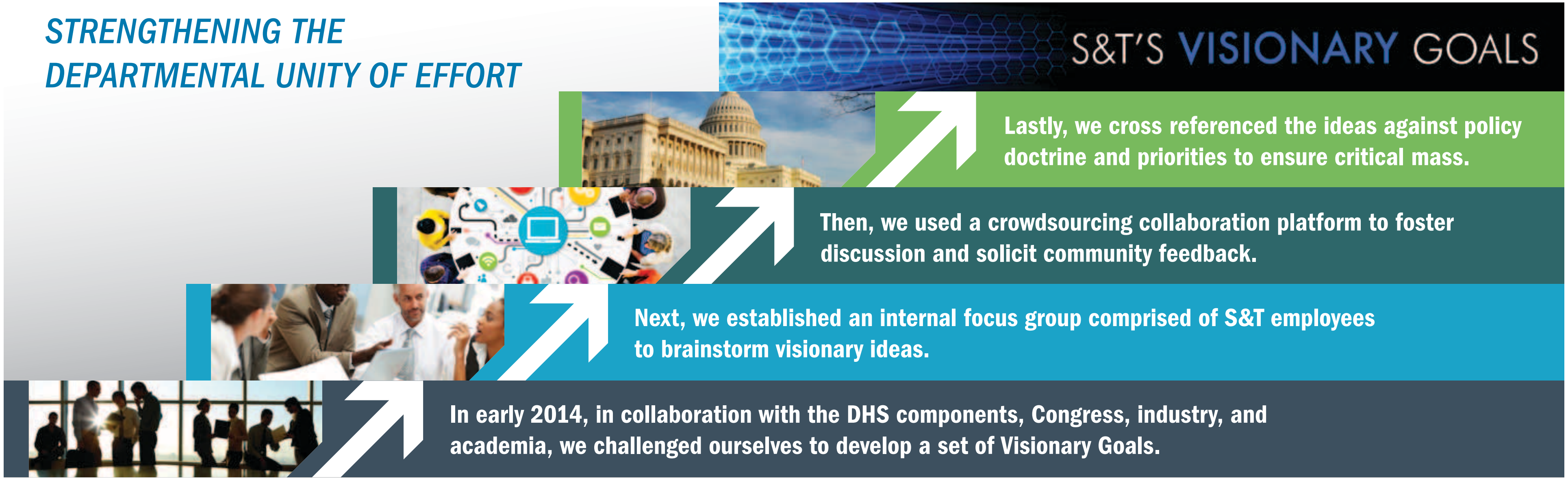


INTRODUCTION AND STRATEGIC CONTEXT CONTINUED

information sharing. These attributes are further complicated by the fact that technology evolution today outpaces federally funded R&D. Therefore, it is critical that S&T develops and sustains effective engagement with the HSIB to capitalize on externally funded investments and innovation. A private sector engine that is well-informed, incentivized, highly agile, and networked can better serve the HSE and improve the overall safety and security of the nation.

In order to achieve the directorate's mission, S&T must establish a strong and healthy leadership culture that recruits, develops, and empowers a 21st-century R&D workforce. To function in the new digital age, the directorate needs scientists who can break down firewalls and are fluent in the language of operators. These "multi-lingual" program managers must be empowered to make risk-informed decisions and manage a balanced R&D portfolio. To equip this workforce with the requisite skills, competencies, and knowledge to advance S&T's mission, the directorate must invest in tools, capabilities, training, and development opportunities.

Finally, it is important to highlight one additional element of S&T's strategic context. To effectively and efficiently address the range of challenges our nation faces, the department recently commenced an initiative entitled "Strengthening Departmental Unity of Effort." In this 2014 memorandum, Secretary of Homeland Security Jeh Johnson directed a series



STRENGTHENING THE DEPARTMENTAL UNITY OF EFFORT

In early 2014, in collaboration with the DHS components, Congress, industry, and academia, we challenged ourselves to develop a set of Visionary Goals.

Next, we established an internal focus group comprised of S&T employees to brainstorm visionary ideas.

Then, we used a crowdsourcing collaboration platform to foster discussion and solicit community feedback.

Lastly, we cross referenced the ideas against policy doctrine and priorities to ensure critical mass.

of actions to create a more cohesive department while preserving the professionalism, skill, and dedication of the people within, as well as the rich history of the DHS components. Pursuant to this guidance, the directorate established Visionary Goals to better unify staff. The goals provide 30-year horizon points to drive innovation within S&T and its ecosystem of technical expertise inside and outside of government.

THE S&T STRATEGY

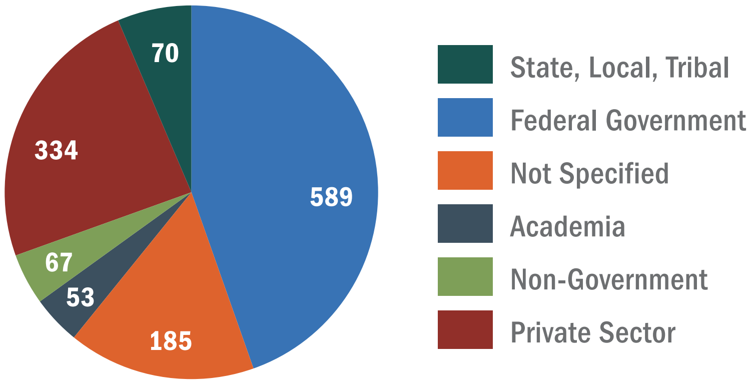
Part II

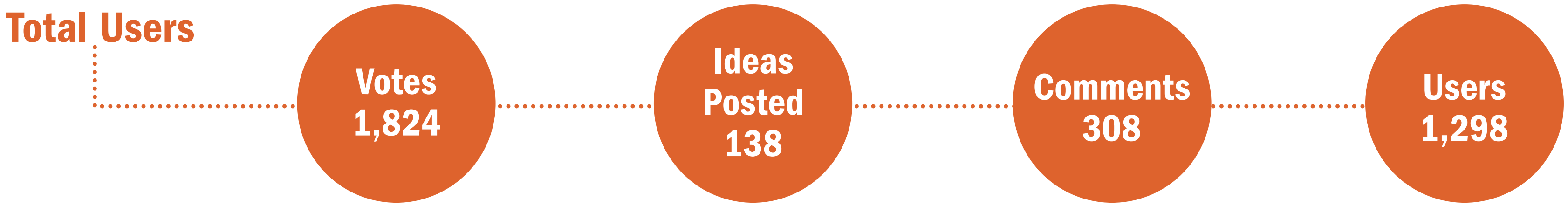
A MORE BALANCED APPROACH

S&T'S VISIONARY GOALS

In order to maximize unity of effort, S&T needed to create Visionary Goals that could unify the directorate and provide strategic direction for years to come. Before developing the Visionary Goals, S&T leaders agreed the goals must satisfy the following requirements: (a) align with DHS doctrine and policy; (b) address strategic challenges and threats prioritized by operators and end users in the HSE; and (c) inspire the science and technology ecosystem to collaborate on and invest limited resources in force multiplying solutions. With these requirements in mind, S&T launched an inclusive, transparent, and dynamic collaboration portal designed to facilitate the development of S&T's Visionary Goals. In the end, nearly 1,300 people within the HSE and HSIB contributed ideas.

BASIC MEMBER DATA
(1,298 Total Users)




Total Users

Votes 1,824

Ideas Posted 138

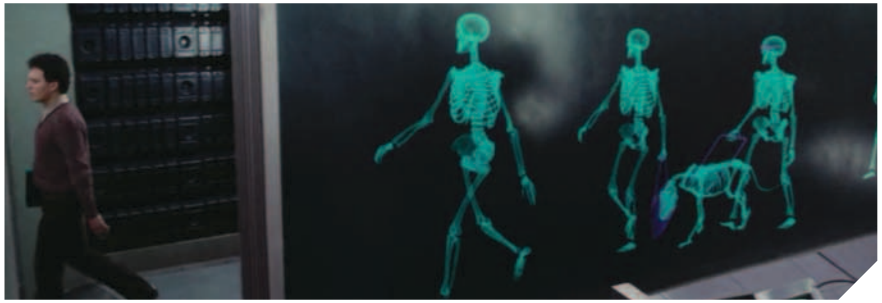
Comments 308

Users 1,298

A MORE BALANCED APPROACH CONTINUED

1990 FILM TOTAL RECALL STILL REPRODUCED WITH PERMISSION.

Based on input from S&T staff, stakeholders, and the public, S&T created the following Visionary Goals, which will serve as S&T's North Star:



REPRODUCED WITH PERMISSION FROM THE 1990 FILM TOTAL RECALL.

Screening At Speed: Security that Matches the Pace of Life

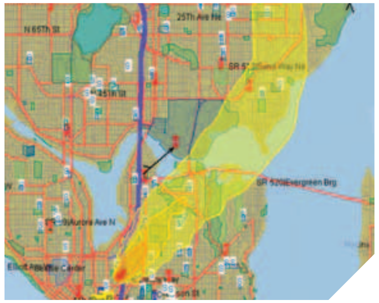
Noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Unobtrusive screening of people, baggage, or cargo will enable the seamless detection of threats while respecting privacy, with minimal impact to the pace of travel and speed of commerce.

A Trusted Cyber Future: Protecting Privacy, Commerce, and Community

In a future of increasing cyber connections, underlying digital infrastructure will be self-detecting, self-protecting, and self-healing. Users will trust that information is protected, illegal use is deterred, and privacy is not compromised. Security will operate seamlessly in the background.

A MORE BALANCED APPROACH CONTINUED

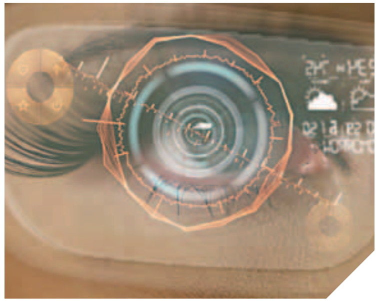
Enable the Decision Maker: Actionable Information at the Speed of Thought



Predictive analytics, risk analysis, and modeling and simulation systems will enable critical and proactive decisions to be made based on the most relevant information, transforming data into actionable information. Even in the face of uncertain environments involving chemical, biological, radiological, or nuclear incidents, accurate, credible, and context-based information will empower the aware decision maker to take instant actions to improve critical outcomes.

Responder of the Future: Protected, Connected, and Fully Aware

The responder of the future is threat-adaptive and cross-functional. Armed with comprehensive physical protection, interoperable tools, and networked threat detection and mitigation capabilities, responders of the future will be better able to serve their communities.



Resilient Communities: Disaster-proofing Society

Critical infrastructure of the future will be designed, built, and maintained to withstand naturally occurring and man-made disasters. Decision makers will know when a disaster is coming, anticipate the effects, and use already-in-place or rapidly deployed countermeasures to shield communities from negative consequences. Resilient communities struck by disasters will not only bounce back, but bounce forward.

THE STRATEGIC FRAMEWORK

DELIVER FORCE MULTIPLYING SOLUTIONS

Given the operational demands on the department and the evolving landscape of threats and natural hazards, S&T must focus its limited resources on delivering force multiplying solutions designed to address the highest priority needs. S&T's framework to achieve this objective involves three interdependent initiatives: (a) identify and prioritize operational requirements and capability gaps; (b) make strategic investments in high-impact, priority areas; and (c) partner with the HSE to increase technology transition, reduce programmatic risk, and repurpose other agency investments. Each of these initiatives emphasizes more collaborative, active, and enduring partnerships with the HSE. By updating its approach to R&D, S&T will cultivate a highly relevant, diversified, and value-creating investment portfolio that delivers force multiplying solutions.

Identify and Prioritize Operational Requirements and Capability Gaps

No matter how big or small, the needs and ideas of the HSE are the seedlings of all current and future R&D at S&T. The directorate leverages numerous sources to collect these operational requirements and capability gaps. Employing a multi-pronged, expedient, and user-friendly approach, S&T actively participates in governance bodies and directly engages with operators. The resulting awareness and understanding of the HSE's operational needs allows S&T to identify cross-cutting requirements, set priorities, and make strategic investments. A few activities that exemplify this initiative include the following:

Departmental and Interagency Governance Bodies – The directorate participates in several standing executive steering committees (ESCs) and councils whose primary purpose is threefold: (a) to communicate requirements and set priorities; (b) to develop strategies and plans; and (c) to manage execution and report on the progress of critical DHS programs. For example, S&T is a critical participant in the DHS Joint Requirements Council (JRC). The JRC is a jointly staffed departmental body tasked with managing portfolio teams chartered to advance the unity of effort goals and objectives set forth by the Secretary of Homeland Security. The portfolio teams focus on critical missions such as cybersecurity; information sharing; chemical, biological, radiological, and nuclear surveillance; aviation security; and information-based screening. S&T's role is to support select portfolio teams with identifying, coordinating, and assessing departmental capabilities, as well as to recommend courses of actions to address gaps. As a result of groups like the JRC, S&T's understanding of operational requirements and capability gaps increases and the directorate is able to propose and implement force multiplying solutions across DHS.

Direct Engagement with Operators – There is no substitution for direct engagement with operators on the frontline of homeland security. Facilitating opportunities for the directorate's scientists, engineers, and program managers to work alongside and communicate directly with the HSE is critical to the success of all projects. The trust built through these relationships and operational insight gained is why S&T continues to invest resources into these activities. Throughout these engagements, S&T employs a systems development life-cycle approach to identify and characterize the operational challenges; design a future state for operations and processes; and conduct test and evaluation activities. Two examples of ways S&T engages with operators are: (a) the Partnering for Innovation and Operational Needs through Embedding for Effective Relationships (PIONEER) program and (b) the First Responder Resource Group (FRRG). PIONEER is comprised of three programs designed to increase the number and depth of relationships between S&T and DHS components. Through participation in

THE STRATEGIC FRAMEWORK CONTINUED

PIONEER's Special Advisor, Exchange Officer, and Embed programs, S&T program managers will experience firsthand a component's operational context and increase their network of operational users. At the same time, the components will gain valuable insight into the directorate's priorities, state-of-the-art technologies, and innovative research. While the PIONEER program focuses on DHS components, the FRRG targets the first responder community. Comprised of active duty and retired first responders, the FRRG is an all-volunteer working group that helps S&T identify the top-priority needs of responders in the field. The group, whose members are drawn from a broad range of disciplines, sectors, and regions of the country, also support the solution development process.

Make Strategic Investments in High-impact, Priority Areas

The directorate's ability to make strategic investments in high-impact, priority areas is dependent upon three prerequisites: (a) the successful execution of activities designed to identify and prioritize requirements, as described in the previous section; (b) the cultivation of a balanced R&D portfolio; and (c) the continued investment in national and directorate capabilities that enable R&D. The latter two prerequisites are described in more detail in the following sections.

Balanced R&D Portfolio

Apex Programs – The strategic focus of S&T's Apex programs is directly linked to our Visionary Goals. Given the complexity and range of issues involved, these high-profile and multidisciplinary programs span three to five years and undergo quarterly reviews by an ESC. Each Apex program consists of a balanced portfolio of projects with scientifically feasible risk that span basic research to advanced technology development. Deliverables range from game-changing technical capabilities to cost-saving business processes. In fiscal year (FY) 2015, S&T dedicated roughly one-quarter of its discretionary R&D budget to eight Apex programs—Air Entry and Exit Reengineering, Border Enforcement Analytics, Border Situational Awareness, Cybersecurity in Critical Infrastructure, Relational Adaptive Processing of Information and Display, Next Generation First Responder, Real-Time Biological Threat Awareness, and Screening at Speed. Through these programs, S&T will tackle the nation's toughest security challenges—both today and in the future—with strategic and innovative solutions.

Technology Engines – A new S&T concept, the Technology Engines are centralized functions that will provide the same suite of services to all Apex programs and to S&T at large; however, they will tailor their work based on a program's individual focus and capability needs. Drawing on the expertise of S&T staff and external scientific, technical, industrial, and academic communities, the Technology Engines will proactively monitor emerging capabilities and state-of-the-art techniques in specific capability areas such as communication and networking tools, data analysis, human systems, and situational awareness. Based on this information, the Technology Engines will provide the Apex programs with best practices, reusable products and solutions, lessons learned, and technical services. The Apex programs will rely on the Technology Engines to produce high-quality solutions that keep pace with advances in the market, ensuring that investments are wisely made.

THE STRATEGIC FRAMEWORK CONTINUED

Innovation and Acquisition – Innovation and acquisition projects are designed to fulfill one of two purposes: (a) to discover breakthrough and disruptive technology that can transition within one to three years or (b) to inform and enable future end-user acquisition programs. In doing so, the innovation and acquisition projects maximize S&T's effectiveness through the research and development of force multiplying solutions. This portfolio involves applied research and advanced technology development.

Quick Reaction – Periodically, S&T receives urgent need statements from end users or inquiries from leadership regarding emerging threats and natural hazards. In these situations, S&T launches quick reaction projects to address these high-priority needs. Working with subject matter experts and leveraging off-the-shelf technologies, S&T aims to deliver capabilities and knowledge products to operators within 12 months.

Capabilities that Enable Research and Development

Capability and Solution Enablers (CaSEs) – For a technology project to be successful, leaders and developers must look beyond traditional R&D activities. Areas such as technology foraging, operational experimentation, technology transfer, commercialization, partnership management, systems analysis, test and evaluation, standards, systems engineering, and solution transition are critical to enhancing the results and outcomes of an R&D effort. Known collectively as CaSEs, S&T provides these enablers to ensure our R&D solutions are better utilized, transition more easily, and can integrate with existing solutions.

Enduring National Capabilities – S&T manages five national laboratories that develop or enhance science, technology, and engineering capabilities. While each has a specific focus—chemical security, biodefense, urban security, animal diseases, and transportation security—the labs work to ensure efforts are coordinated, are not duplicative, and support investments in high-impact, priority areas.

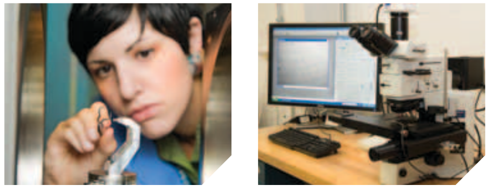
S&T'S FIVE NATIONAL LABORATORIES

Chemical Security Analysis Center

National Urban Security Technology Laboratory

National Biodefense Analysis and Countermeasures Center

Plum Island Animal Disease Center



Transportation Security Laboratory

THE STRATEGIC FRAMEWORK CONTINUED

Partner with the Homeland Security Enterprise

S&T must continuously invest in the creation and maintenance of partnerships with DHS components and other R&D organizations. Internal and external partnerships are a core element of our strategy and serve as the foundation of S&T's innovative ecosystem. Whether through international agreements with allied foreign nations, grants to academic institutions, or Cooperative Research and Development Agreements with industry, S&T continually pursues new opportunities and instruments to formalize relationships with innovative organizations. Benefits from these partnerships are numerous and include diversifying investments across a broader range of operational needs, increasing technology transition, reducing programmatic risk, and leveraging other agency investments. In turn, these benefits position S&T to have the financial and analytical resources to deliver force multiplying solutions. The following activities highlight the execution of this initiative:

Innovation Centers – The Innovation Centers aim to transition capabilities to end users through cutting-edge R&D projects. Owned and operated by the DHS components, the centers will be jointly funded and staffed by S&T to provide R&D support. The Innovation Centers perform three critical functions that complement S&T's mission space and strategy: (a) coordinate internally funded component research with related S&T and DHS projects; (b) enable and/or execute technology transition activities such as late-stage technology development, rapid prototyping, and test and evaluation; and (c) foster an innovative and entrepreneurial culture that inspires new ideas, promotes stakeholder engagement and transparency, and cultivates an enduring ecosystem focused on solving critical homeland security challenges.

In-Q-Tel (IQT) – IQT serves as a bridge between federal agencies and start-up firms on the leading edge of technological innovation. In 2011, S&T formalized a strategic partnership with IQT. Pooling resources from nine federal agencies, IQT identifies, adapts, and delivers innovative technologies that solve some of the department's highest priority operational needs at a fraction of the cost. In fact, for every $1 invested by S&T we have leveraged $2.66 from other U.S. government agencies; as a result, S&T has been able to partner with the HSE for an even greater impact and return on investment.

Federal Partners – S&T partners with other federal R&D organizations to develop innovative and game-changing solutions to advance the homeland security mission. As part of this effort, S&T maintains strong partnerships with national laboratories, such as those of the Department of Energy and Department of Defense, and reaches out to other partners in areas such as agriculture, environment, health, and transportation.

Academia – S&T partners with the nation's colleges, universities, and leading academic researchers to develop customer-driven, innovative tools and technologies that solve real-world challenges, as well as to train the next generation of homeland security professionals. As part of these efforts, S&T funds 10 Centers of Excellence (COEs) that address specific homeland security challenges. For example, the newest COE—the Critical Infrastructure Resilience Center—will conduct research to understand how businesses determine acceptable risks; develop scalable, cross-sector solutions that meet national needs; pilot solutions in the real world; and prepare business cases for investing in resilient critical infrastructures and systems.

THE STRATEGIC FRAMEWORK CONTINUED

ENERGIZE THE HOMELAND SECURITY INDUSTRIAL BASE

Unlike many other industries with well-defined sets of products, technologies, and customers, the HSIB is a highly fragmented federation of product and service providers serving a broad constituency. Customers and their needs vary widely, from ships for the U.S. Coast Guard to protective gear for first responders to cyber defense tools for power plants. This degree of fragmentation means that many companies with leading-edge technologies are often small and more challenging to locate and engage. Simultaneously, federal, state, and local agencies are spending less on R&D for next-generation technologies. Therefore, it is critical that S&T collaborate with the HSIB to capitalize on industry investments in R&D and encourage the development of force multiplying solutions that defend, defeat, and mitigate threats to the nation.

In order to energize the HSIB, S&T will revamp existing programs so industry can more easily partner with S&T. We will also develop new approaches to engage non-traditional companies. The following initiatives highlight specific activities that will help us achieve this objective.

Optimize Markets by Pooling Demand and Developing Standards

Our partners around the globe share a common mission—to ensure the safety and security of the people they serve. Most countries collaborate at an international level but largely address their challenges independently; as a result, they have limited funding to handle complex challenges and often create duplicative efforts or struggle to gain traction in a fragmented global market. S&T is working to integrate markets with international partners to draw down industry risks and incentivize product development. S&T is also working with the HSIB to consolidate R&D investments, pool demand, and accelerate the development of standards. This will improve the interoperability of technology and allow the HSIB to better plan and reduce costs. The following activities highlight the execution of this initiative:

International Engagement – S&T is in the process of creating the International Forum to Advance First Responder Technology. The forum will serve as an international platform to discuss responder challenges and issues. Responders will be able to partner on R&D initiatives through the forum and, when possible, align procurements to drive industry investments in innovative technologies and manufacturing capabilities. The forum will give responders a global voice and use common challenges and standards to create or broaden global markets for first responder technologies. Ultimately, this lowers risk for industry and incentivizes investment in more robust capabilities and product lines.

Standards Development – S&T plays a leading role in accelerating the development of standards for use by the HSE. Standards are vital in establishing best practices, achieving interoperability, supporting acquisitions, and defining grant guidance. In an effort to achieve earlier adoption of standards and inclusion in commercial products, S&T will engage industry throughout the standards development process. This approach will ensure that technologies from different manufacturers can interoperate through the use of open-source, non-proprietary solutions and standards-based approaches. Today, S&T is working on both information technology standards and physical standards.

THE STRATEGIC FRAMEWORK CONTINUED

Engage the HSIB through a Deliberate, Continuous, and Transparent Approach

S&T brings together interested parties—including responders, operational users, citizens, and academia—to engage the HSIB. Working together, each community plays a critical role in shaping the future of homeland security technology. S&T is launching new outreach mechanisms, such as online forums, to foster understanding of the homeland security market and build progress toward outcomes that will keep us all safer and minimize disruption to the pace of daily life. Additionally, S&T will use new funding vehicles like prize competitions to attract innovators who have not historically partnered with the federal government. The following activities highlight the execution of this initiative:

National Conversation on Homeland Security Technology – S&T is initiating idea exchange between operational users within the HSE and industry-based technologists. Using an online, open platform and in-person discussions, S&T is enabling end users to connect directly with technology developers. The goal of these discussions is to help industry better understand the homeland security market and create innovative and sustainable homeland security solutions.

HSIB Research and Development Coordination – S&T is exploring ways to better coordinate R&D across the HSIB, including with large commercial manufacturers and small businesses with niche capabilities. Improving coordination with this diverse community of industry partners will provide S&T insights into emerging technologies and how they can fill capability gaps. Further, S&T will work with private sector partners on rapid prototyping and identify lessons learned to better foster innovation.

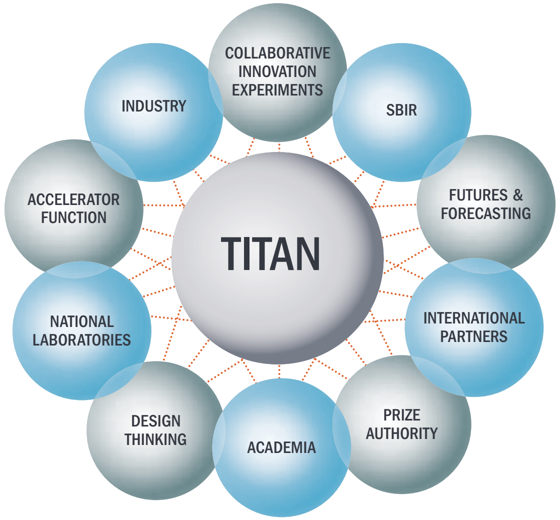
Outreach Mechanisms Designed to Engage Non-traditional R&D Performers –
The landscape of technology R&D is changing as federal agencies and large corporations are no longer the dominant driver of innovation. Increasingly, advances are being discovered, developed, and distributed by non-traditional performers across every technology space. However, many of these non-traditional performers do not consider federal agencies as a potential customer market or source of funding because of the resource-intensive nature of doing business with the government. To ensure that the HSE remains on the cutting edge of technology capability, S&T must employ new methods to engage these non-traditional performers. In this regard, S&T leverages key partnerships with trade associations, innovation and start-up foundations, accelerators, incubators, the venture capital community, and entrepreneur groups to engage non-traditional partners. In partnership with these key hubs, S&T will lead interactive workshops with new communities to discuss homeland security needs that may drive technology development. S&T will also encourage new ideas from industry by launching prize competitions. Teams of companies, students, and hobbyists will be able to compete to provide viable and marketable solutions for prize funding. Additionally, S&T will host hackathons where technology developers come together to tackle a homeland security challenge in a rapid, iterative, and collaborative way. We also aim to become a leader in the broader technology scene by hosting innovation talks on scientific, cultural, and academic topics. An example of such innovative series of talks are *TED Talks*™ run by the Sapling Foundation and *Virgin Disruptor* discussions run by the Virgin Group. The goal with each of these efforts is to bring new energy, resourcefulness, and ideas to the homeland security landscape.

THE STRATEGIC FRAMEWORK CONTINUED

Improve Programs Designed to Increase Collaboration with Innovative Companies

S&T and the HSIB exist in an environment of rapidly evolving threats and opportunities, and the accelerating pace of risk and technological development loom over every mission in the department. U.S. government funding remains a strong influence on basic research, but private sector investment focused on late-stage development surpassed the government's total annual R&D investments in the 1980s and has continued since then. In homeland security, innovation cycles in areas like advanced analytics, communications, additive manufacturing, and cybersecurity occur so quickly that traditional government vehicles for investment and acquisition struggle to keep up with advances and changes in technology. In order to leverage these accelerated advancements, S&T will revamp existing programs so industry can more easily partner. S&T is seeking ways to engage the investor community with an accelerator component. This program will provide S&T with insight into a range of innovation companies that can provide near- and long-term capabilities. S&T will reengineer our technology foraging approach and add a forecasting component to capitalize on industry investment trends and influence emerging technology. S&T will establish close working relationships with innovators to reduce development risk and facilitate early evaluations of solutions by operational users. S&T will also provide a flexible environment for validating and guiding the development of game-changing products and services as they approach market readiness. The following activities highlight the execution of this initiative:

Targeted Innovative Technology Acceleration Network (TITAN) – Using an arsenal of engagement tools, TITAN seeks to discover and engage innovators who are creating technologies that will enable homeland security operators to carry out their missions in new, unprecedented ways. TITAN will unify and coordinate formerly disparate activities within S&T into a cohesive program for engaging the HSIB. TITAN removes barriers that impede industry partners from working with S&T. TITAN also seeks pathways for S&T to work with industry and small businesses in a more synchronized, strategic fashion to improve the pace and quality of solution development.



TARGETED INNOVATIVE TECHNOLOGY ACCELERATION NETWORK

Responder Technology Alliance (RTA) – Through unique, strategic partnerships with first responders, the industry and investment community, and R&D organizations, RTA is tackling the most difficult and complex responder challenges. RTA will take a systems-based life-cycle approach to first responder technologies, integrating industrial design, systems engineering, cost and supply chain analysis, and market assessment. RTA is developing short-, mid-, and long-term scalable solutions that can be integrated into responder operations to strengthen

THE STRATEGIC FRAMEWORK CONTINUED

responders' health, safety, and effectiveness. Further, RTA is leading an accelerator program to create solutions at market speed. Individuals or small companies with promising solutions will be able to work directly with angel investors, venture capitalists, and responder equipment manufacturers to increase their odds of commercial success.

ESTABLISH A STRONG AND HEALTHY LEADERSHIP CULTURE

S&T's ability to achieve the aforementioned strategic objectives depends upon a common identity, clarity of mission, and leadership at all levels of the organization. With empowerment, responsibility, and accountability as cultural values, S&T strives both to create an innovation-friendly environment and to give staff the tools and development opportunities to grow and succeed within it. S&T's work environment will be educational and entrepreneurial. The workforce will be agile, inquisitive, and eager to find and execute new ideas, take informed risks, and engage external partners. To instill this culture, S&T will focus on three initiatives: (a) empower the workforce; (b) provide meaningful leadership development and professional growth opportunities; and (c) engineer a pipeline for the next generation of homeland security professionals.

Empower the Workforce

Empowering the workforce means giving a stronger voice to S&T staff and fostering a broader sense of ownership and attachment to the organization. S&T values our workforce's perspective and believes that none of us individually is as smart as all of us collectively. Moving forward, leadership will continue to integrate staff input into initiatives that affect the immediate and long-term course of the organization, such as the National Conversation on Homeland Security Technology. The following activities are intended as platforms for S&T employees to influence the organization's direction:

Employee Council – S&T will charter its inaugural Employee Council to act as a voice for S&T's workforce. Comprised of federal non-supervisory representatives, the council will identify and communicate employee perceptions on S&T programs and policies and discuss issues faced by the S&T workforce. Through the council, S&T staff will advise senior leadership on these issues and make recommendations on potential solutions. The council's recommendations and communication with senior leadership will be transparent and available to the entire workforce. The council will foster more open and clear communication between leadership and staff and ultimately make S&T's workforce more invested in the organization.

Broadening S&T Decision Making – In addition to giving staff a greater say over S&T's programs, the Under Secretary has made it a priority to decentralize decision making and delegate certain authorities to managerial levels throughout the organization. This will have the dual effect of minimizing bottlenecks for decisions that can be made at lower levels and expanding ownership of S&T's strategic direction. Examples of supporting efforts include the Apex ESC and the Project Prioritization process. The Apex ESC oversees the planning and execution of the Apex programs and Technology Engines. Chaired by each of S&T's group leads, the ESC reviews, approves, and provides resources for the Apex programs and

THE STRATEGIC FRAMEWORK CONTINUED

serves as the primary liaison between Apex efforts, S&T staff, and the Under Secretary. In the Project Prioritization process, representatives from across the directorate review and prioritize S&T's research, development, and innovation investments—first independently and then collectively—before presenting their recommendations to S&T leadership for approval.

Provide Meaningful Leadership Development and Professional Growth Opportunities

To arm our workforce with the skills, competencies, and knowledge to advance S&T's mission, the directorate must invest in tools, capabilities, training, and workforce development opportunities. Our robust program, which includes relevant courses at universities and colleges, encourages employees to enhance their R&D, leadership, and management skills. Specific activities to support this initiative include the following:

Assessments – S&T offers a broad range of assessments to help staff members better understand how they think and behave and how that affects them in the context of their work environment. These include 360-degree reviews and numerous popular private-sector offerings that not only improve self-awareness but also give managers tools to increase team productivity and cohesion.

Assessments
Internal Opportunities Network
Leadership Development
Apex Training Program

Internal Opportunities Network – S&T has created a Web-based portal to advertise short-term developmental assignments within S&T and DHS to enhance employees' careers. Exposing our workforce to new experiences within the directorate and the department helps our staff develop new abilities, expertise, and relationships outside their home office.

Leadership Development – S&T offers several opportunities for leadership development, including a coaching program and leadership cohort. These opportunities emphasize personal accountability and teach participants how to model leadership through one's actions and how to create a vision.

Apex Training Program – S&T developed a unique training program for Apex program managers and team members to learn best practices and lessons learned from the original four Apex programs. Following the training program, participants understand how to use all of the organization's tools to support the execution of an Apex program.

THE STRATEGIC FRAMEWORK CONTINUED

Engineer a Pipeline for the Next Generation of Homeland Security Professionals

To ensure that the directorate continues to build on successes and evolve to meet new challenges, S&T is committed to growing a pipeline for S&T's next generation of staff. Part of this effort includes continuously assessing the organization and performing a forward-looking analysis of where staff needs will grow or decline. Based on this data, S&T will determine what expertise is needed to support S&T's mission and make long-term investments in those areas to ensure that appropriate hires are prepared to join S&T. The following two activities describes S&T's efforts to plan and develop its future workforce:

Strategic Workforce Planning – S&T will develop an enduring institutional capability to ensure projects and teams are properly resourced. This planning effort will continuously assess S&T's workforce requirements, taking into account S&T's complex mission, unique staff requirements, and the operational demands of today as well as the forecasted needs of tomorrow. S&T will also assess internal workforce-related business processes and use of hiring authorities in order to eliminate unnecessary delays while still ensuring compliance with appropriate rules and regulations.

Sourcing Talent More Effectively – As S&T begins to plan and shape its workforce more effectively, we will begin adding or connecting to talent that fills described gaps or enriches efforts already underway. This initiative will require S&T to more effectively and efficiently interface with non-government sources of expertise, build on existing relationships (e.g., use of American Association for the Advancement of Science fellowships), and take advantage of DHS's full range of career and term-limited hiring authorities. As S&T becomes more transparent and public-facing, for example through our updated website and more informative Internet presence, we will also expand our ability to connect to outside expertise.

Shaping S&T's Next Generation – Faced with rapidly accelerating technologies and increasingly complex homeland security threats and challenges, S&T must prepare a future workforce that is capable of delivering specific competencies as new needs emerge. S&T will leverage its significant investment in universities to ensure a pipeline of young new employees. S&T's 10 COEs, along with our Minority Serving Institution grants and awards programs, will engage thousands of students directly in homeland security-specific coursework, scholarships, fellowships, and research opportunities. S&T will also continue to use career development grants, summer internships, and summer research teams to develop needed staff and skill sets for the future.

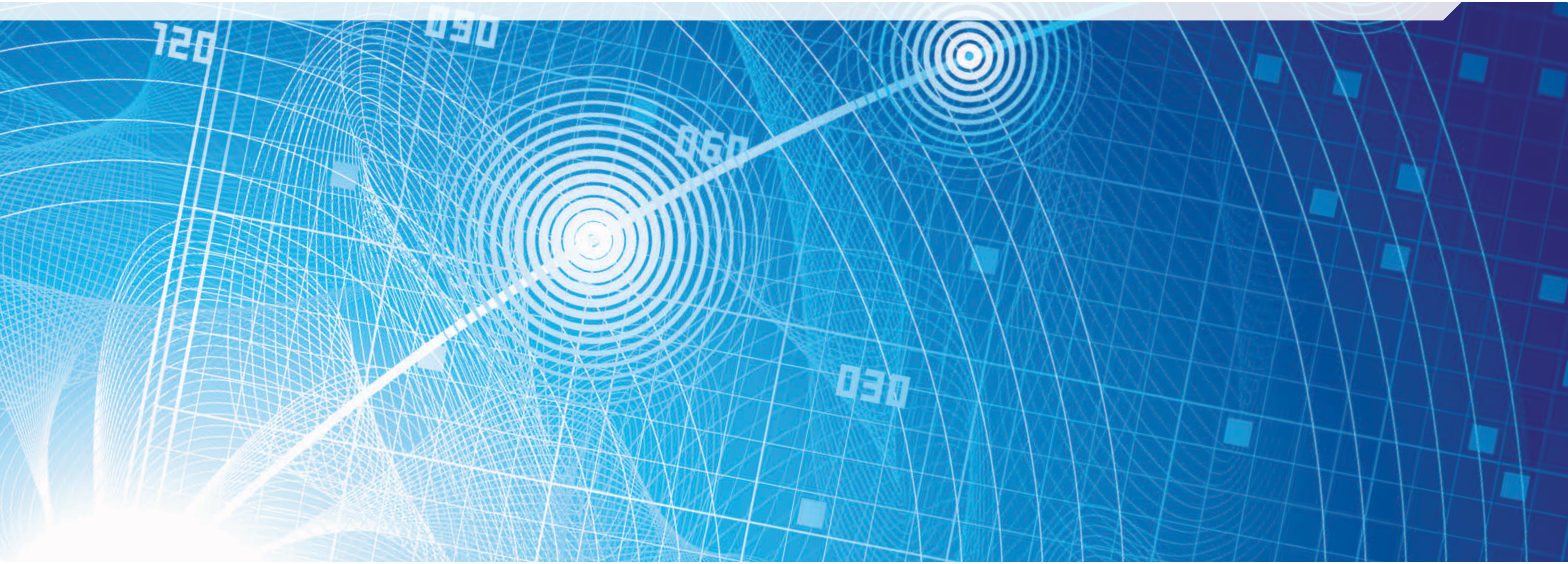
IMPLEMENTATION PLAN

S&T STRATEGIC FRAMEWORK			Intensity of Activity (FY 2015 FY 2019)				
			FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Deliver Force Multiplying Solutions	I	Identify and Prioritize Operational Requirements and Capability Gaps	▨	■	■	■	▨
	II	Make Strategic Investments in High-impact, Priority Areas	■	■	■	■	■
	III	Partner with the Homeland Security Enterprise	▨	■	■	■	▨
Energize the Homeland Security Industrial Base	I	Optimize Markets by Pooling Demand and Developing Standards	■	■	▨	▨	▨
	II	Engage the HSIB through a Deliberate, Continuous, and Transparent Approach	▨	■	■	■	■
	III	Improve Programs Designed to Increase Collaboration with Innovative Companies	■	■	■	▨	▨
Establish a Strong and Healthy Leadership Culture	I	Empower the Workforce	■	■	■	■	■
	II	Provide Meaningful Leadership Development and Professional Growth Opportunities	▨	■	■	▨	▨
	III	Engineer a Pipeline for the Next Generation of Homeland Security Professionals	■	■	▨	▨	▨

Color Legend	Intensity Levels
Surge Effort	■
Steady-state Effort	▨

S&T's implementation plan is phased over the next five years with specific levels of effort committed to the objectives, initiatives, and activities outlined in this strategic plan. Efforts committed in the first few years are designed to finish planning, including key actions and success measures, and jump-start activities designed to enable future related efforts. S&T is committed to remaining on track with the implementation plan. Quarterly reports will be provided to S&T leadership in order to assess the directorate's progress against key actions. Using this information, S&T leadership will reexamine the strategic plan on an annual basis and make any required course corrections.

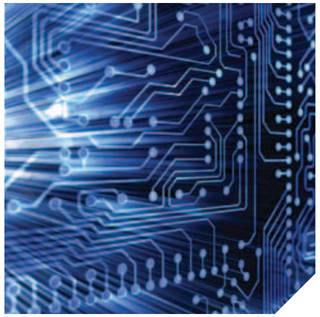
RESEARCH & DEVELOPMENT STRATEGIC PRIORITIES



Part III

RESEARCH & DEVELOPMENT STRATEGIC PRIORITIES

S&T sets R&D priorities through participation in governance bodies and discussions with mission owners. Once an investment decision has been made, S&T engages the whole of government and HSIB in order to develop a Capability Roadmap. Each of the five S&T Homeland Security Advanced Research Projects Agency (HSARPA) divisions, the three First Responders Group divisions, and Apex programs and Technology Engines have developed Capability Roadmaps aligned to the needs of their operational end users. These high-level roadmaps formalize a vision, identify strategic drivers, and list R&D objectives for the next five years. The roadmaps are constantly evolving documents and serve three primary organizational functions: (a) to build consensus among a diverse set of end users with similar operational requirements; (b) to develop a framework that directly links a strategy to tactics; and (c) to provide a framework to coordinate planning, research, development, and acquisition activities across the various groups involved.



HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS

Borders and Maritime Division (BMD)

Vision – Our long-term vision is to create a single Border and Coastal Information System (BACIS) that provides a border security information sharing environment. The BACIS will allow users to share data and tools across the entire HSE and will encompass all borders and transportation modes, including the northern and southern land borders, the coastal/maritime border, cargo and vehicles at the Ports of Entry (POEs), and people at the POEs.

Strategic Drivers – BMD's future efforts will be guided by 2014 Quadrennial Homeland Security Review (QHSR) Mission 2: Secure and Manage our Borders (specifically goals 2.1, 2.2, and 2.3), 2014 QHSR Mission 3: Enforce and Administer our Immigration Laws (specifically goal 3.2), and S&T's Visionary Goals of "Screening at Speed: Security that Matches the Pace of Life" and "Enable the Decision Maker: Actionable Information at the Speed of Thought." BMD's efforts will also be influenced by the 2014 QHSR's strategic aim to Mature and Strengthen Homeland Security by focusing on (1) integrating intelligence, information sharing, and operations; (2) enhancing partnerships and outreach; and (3) by conducting Homeland Security Research and Development. In addition, the execution of BMD's research will focus on (1) operations, innovation, and partnerships, specifically by transitioning mature and rapidly deployable solutions to DHS operational components; (2) developing technologies that have a positive impact on operations and return on investment for our customers; (3) collaborating with DHS components, other government agencies, and international partners to reduce R&D costs and time to delivery; and (4) partnering with industry to transition new technologies and guide their investments.

Description of Capabilities:

- **Land Border Security** – Develop and transition technical capabilities that strengthen U.S. land border security by safeguarding lawful trade and travel and helping to prevent illegal goods and people from crossing the border.
- **Maritime Border Security** – Develop and transition technical capabilities that enhance U.S. maritime border security by safeguarding lawful trade and travel and preventing illegal use of the maritime environment to transport illicit goods and people.
- **POE Security** – Develop and transition technologies to ensure the integrity of people and cargo that enter the United States through the POEs, including seaports, airports, and land border crossings. Enhance the end-to-end security of the supply chain, from the manufacturer of goods to final delivery, while ensuring economic throughput for the U.S. economy.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Land Border Security				
Perform operational assessments of small unmanned aerial systems (SUAS) for improved detection, identification, and classification of illicit activity and improved situational awareness in land operational scenarios. Publish reports. Transition the Slash CameraPole (one-pole configuration) to U.S. Customs and Border Protection (CBP). Install a three-pole configuration and commence operational assessments. Transition the Southwest Border Buried Tripwire to CBP. Transition a lab developmental prototype of the Tunnel Age Kit to U.S. Immigration and Customs Enforcement (ICE).	Transition the Moving Target Indicator capability to CBP. Transition the Automated Scene Understanding/Canadian-U.S. Sensor Sharing Pilot capability to CBP. Transition (System 1) Unattended Ground Sensors to CBP. Field test a lab developmental prototype of the Tunnel Detection System. Field test Tunnel Age Kits.	Transition (System 2) Unattended Ground Sensors to CBP. Transition a three-pole configuration of the Slash CameraPole to CBP. Transition Low Rate Initial Production Tunnel Age Kits, a test report, and technical data to ICE.	Transition Radio Frequency Sensing Unattended Ground Sensors to CBP. Transition a prototype, test report, and technical data for the Tunnel Detection System to CBP.	Deliver a final prototype of the Tunnel Detection System and technical data to CBP's Office of Innovation and Technology Acquisition. Transition technologies to detect, locate, and disrupt border spotters employed by traffickers along the Southwest border to CBP. Transition technologies and tools to increase the safety and effectiveness of HSE operational end users.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Borders and Maritime Division (BMD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Maritime Border Security				
Install Coastal Surveillance System (CSS) operational nodes at strategic locations to improve U.S. maritime domain awareness. Perform operational assessments of SUAS for improved detection, identification, and classification of illicit activity and improved situational awareness in maritime operational scenarios. Publish reports.	Transition Integrated Maritime Domain Environment to DHS as an enterprise. Perform CSS operational demonstrations. Install CSS operational nodes at additional locations to improve U.S. maritime domain awareness. Continue to perform operational assessments of SUAS in maritime operational scenarios. Publish reports.	Transition the CSS initial operating capability to the Joint Task Force, Air and Marine Operations Center, and the U.S. Coast Guard (USCG). Install CSS operational nodes at additional locations to improve U.S. maritime domain awareness.	Deliver to DHS an integration platform for agile information sharing and discovery. Deliver to CBP; USCG; and state, regional, and local partners a coastal maritime sensor fusion system that enables cooperative maritime awareness of non-emitting vessels and the sharing of time-critical, mission-useful sensor information.	Integrate CSS into USCG's Watchkeeper system. Transition technology to enhance the utilization of SUAS in the maritime domain.
Objective: Ports of Entry Security				
Finalize the United States–European Union (US-EU) Maritime Cargo Security Pilot Test Plan and preliminary assessment of the efficacy of various cargo security devices for use in the US-EU. Conduct a maritime cargo security pilot. Conduct an end-to-end analysis that will influence electronic chain-of-custody processes, procedures, and technology implementations. Complete CBP maritime and truck demos and Phase II Federal Protective Service demos of the government Reusable Electronic Conveyance Security Device. Develop a Border Wait Time/Supply Chain Security Roadmap. Pilot border wait time technologies.	Transition to CBP and FPS a test and evaluation analysis, a cost/benefit analysis, acquisition recommendations, and a vendors list of piloted RECONS. Transition to CBP and the governments of Mexico and Canada guidelines for the use of commercial RECONS. Transition proven border wait time technologies. Deliver the Polymerase Chain Reaction collection efficiency technology to CBP. Deliver a pollen forensic technology to CBP.	Deliver the Mobile Backscatter Scanning System upgrade to CBP. Deliver the Conveyance Void Anomaly Detector to CBP. Deliver currency detection technologies to CBP. Deliver invasive species detection technologies to CBP. Deliver counterfeit goods detection technologies to CBP.	Deliver to DHS law enforcement agencies (e.g., CBP, ICE) a secure communications and database architecture to enable law enforcement officers to access and share information securely.	Deliver an enhanced pollen forensic technology to CBP. Deliver an enhanced Polymerase Chain Reaction collection efficiency technology to CBP.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Chemical and Biological Defense Division (CBD)

Vision – CBD's work will enable society to be resilient to events involving chemical and biological agents through rapid awareness of the release of agents, effective response guidance, and efficient recovery of infrastructure.

Strategic Drivers – Multiple Presidential directives and national security strategies rely on knowledge, technologies, and guidance from DHS to ensure national readiness and preparedness for chemical and biological threats. To counter the threats ahead, CBD is taking into consideration the following strategic drivers:

- An increasing array of emerging threats added to long-recognized agents enhances the complexity of the threat landscape.
- Informed assessment of the risks posed by the threat landscape is required to allocate resources wisely.
- A national biosurveillance strategy places a premium on the integration of data from multiple sources, including public health and environmental sensors, to enable rapid, well-informed decisions to reduce exposures and minimize contamination spread.
- Advancing detector technology must recognize cost-related barriers to implementation.
- The broad set of potential causative agents of disease requires innovation in assay development to recognize more agents with fewer assays and extend to identifying agents that may presently be unknown.
- Demonstrating recovery technologies in operational environments in concert with local, state, and national response entities is essential to developing guidance that can be readily absorbed by and transitioned to those entities.

Description of Capabilities:

- **Threat Awareness** – Develop and promote risk-based approaches to inform effective prevention, preparedness, and response and recovery actions to biological and chemical terrorism events.
- **Surveillance, Detection, and Diagnostics** – Promote information integration and real-time situational awareness to reduce agent spread and enable early actions to minimize consequences to people and property. Develop trusted tools for the rapid identification and confirmation of a threat to guide appropriate response actions.
- **Response and Recovery** – Develop and incorporate a range of activities that enhance the return to normalcy after a chemical or biological contamination or animal disease event, such as developing decontamination technologies and guidelines, environmental sampling and testing methodologies, requirements for key infrastructure, and broad-spectrum medical countermeasures to halt the transmission of animal diseases.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Threat Awareness				
Complete material threat assessments for priority agents in concert with interagency partners. Refine the Countermeasure Assessment and Planning Tool and pilot with interagency partners.	Deploy the Bio Knowledge Management System to all Fusion Centers. Deliver updated biological, chemical, and integrated risk assessment reports. Complete field tests of large-volume releases of chlorine.	Establish an independent S&T risk assessment modeling repository. Deliver a new chemical hazards knowledge management system. Deliver the 2017 Integrated Terrorism Risk Assessment.	Deliver risk mitigation studies to DHS stakeholders for resource allocation in chemical, biological, radiological, and nuclear defense. Deliver the 2018 Biological Terrorism Risk Assessment and brief stakeholders to maximize awareness and utility of the product.	Develop an understanding of new defense capabilities that may reduce the risk and influence of biodefense investments. Deliver the 2019 Integrated Terrorism Risk Assessment.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Chemical and Biological Defense Division (CBD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Surveillance, Detection, and Diagnostics				
Complete test, evaluation, and, validation of rapid real-time polymerase chain reaction (PCR), antigen, detection/diagnostics assays, and hand-held first responder assays for several Tier 1 priority agents. Initiate a demonstration project in select locations to further develop biosurveillance requirements.	Demonstrate the feasibility of low-cost, sustainable environmental detection architecture. Complete development of rapid detection assays for Tier 1 priority agents and rapid anti-microbial tests for priority bio agents.	Conduct a full-scale biosurveillance exercise in concert with public health and response communities. Transition validated, laboratory-based real-time PCR and antigen/toxin detection assays for high consequence (Tier 1) viral and bacterial agents to the Centers for Disease Control and Prevention (CDC) Laboratory Response Network (LRN) for deployment.	Demonstrate analytics of disparate data relevant to biosurveillance objectives. Transition validated, laboratory-based real-time PCR and antigen/toxin detection assays for Tier 2 bacterial threat agents to the CDC LRN for deployment.	Complete transition of validated, laboratory-based real-time PCR and antigen/toxin detection assays for Tier 2 bacterial viral and toxin threat agents to the CDC LRN for deployment. Conduct independent test and evaluation of a detection system for surface transportation security.
Objective: Response and Recovery				
Initiate evaluation of decontamination technologies and advanced sampling and analysis techniques to expedite the recovery of a bio-contaminated subway system.	Complete a draft interim guidance document for subway recovery. Develop analytical standards for whole genome sequencing to aid forensics.	Issue final guidance on the restoration of underground transportation systems after a biological incident. Identify common viral targets to enable construction of a foot-and-mouth disease panvalent vaccine.	Complete the first year of an international field trial of foot-and-mouth disease vaccines and diagnostics.	Demonstrate in vitro efficacy of a broad spectrum of agricultural bio-therapeutic candidates.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Cyber Security Division (CSD)

Vision – CSD strives to create an HSE cyber infrastructure that is secure from cradle to grave. Secure, in this context, is defined by the following set of properties: trustworthy, dependable, robust, survivable, transparent, observable, privacy-regulated, self-aware, and self-adaptable.

Strategic Drivers – The S&T Visionary Goal "A Trusted Cyber Future: Protecting Privacy, Commerce, and Community" and the 2014 QHSR goals 4.3 and 4.4 will guide CSD's research in the years to come. CSD will aim to improve the underlying infrastructure of the digital world and ensure information is protected, illegal use of information is deterred, and privacy is not compromised. Primary technological and threat drivers include:

- The continued growth of the Internet of Things, which will result in heretofore unconnected devices interacting via the Internet.
- The interconnection of multiple aspects of life (e.g., critical infrastructure, medical devices, automobiles) that depend on digital devices and information. As this continues to expand, the impacts and consequences of these connections will become increasingly difficult to predict.
- The barriers to entry for cyber criminals, "hacktivists," and cyber terrorists will decrease, expanding the pool of those who can disrupt the cyber infrastructure.

Policy directives and implementation will also continue to impact CSD's research portfolio. Recent legislation and executive orders have, for example, established requirements for a National Critical Infrastructure Security and Resilience (CISR) R&D plan (Presidential Policy Directive-21), launched a cyber-threat intelligence integration center, and called for a Federal Cybersecurity R&D plan (Cybersecurity Enhancement Act of 2014). Policy, however, will continue to lag behind technology advances, thus creating seams or gaps in the regulation and enforcement of cybersecurity norms and development of technical solutions.

Description of Capabilities:

- **Cybersecurity Research Infrastructure** – Provide the infrastructure necessary to support cyber R&D in order to match growing and adapting threats. Make special testbeds and data sets available to the cyber research community, so researchers and developers can safely test malicious code somewhere other than on the live Internet or on real data.
- **Software Assurance** – Develop innovative approaches to reduce the risk and cost of software failures. Create new tools and techniques to improve the ability of software developers to analyze software for potential vulnerabilities. Apply new test and evaluation capabilities to correct vulnerabilities and reduce the probability and frequency of exploitation.
- **Network Security** – Define and develop network and system security metrics and techniques for mapping and modeling the networks, systems, and services that comprise the Internet, so as to better understand the Internet's evolving structure and vulnerabilities.
- **Mobile, Web, and Cloud Security** – Develop technologies and approaches to secure networks, systems, and their constituent devices, including mobile devices, the Web, and the cloud.
- **Identity Management and Privacy** – Develop interoperable access control technologies to provide federal, state, and local government agencies with a cost-effective way to share information without compromising the privacy of individuals (i.e., personally identifiable information) or organizations.
- **Cybersecurity Education and Training** – Improve the quality and skill set of the next generation of cybersecurity professionals by exposing students to the latest defense technologies in a competitive environment. Improve the performance and skills of Cyber Security Incident Response Teams (CSIRTs).
- **Securing Critical Infrastructure** – Protect owners, operators, and users by developing and delivering technologies across industry, government, the private sector, and academia to improve the core functions of critical sector information systems and control systems.
- **Transition to Practice** – Identify innovative, federally funded research cybersecurity research that addresses existing or imminent cybersecurity gaps, fund necessary improvements identified during pilot programs and test and evaluation activities, and transition this research into the HSE through partnerships and commercialization.
- **Cybersecurity for Law Enforcement** – Develop new technologies, capabilities, and standards to assist law enforcement in conducting investigations and forensic analysis of technologies used in criminal activity. Aid organizations in mitigating the potential impact and damage posed by insider threat activity.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Cybersecurity Research Infrastructure				
Create a legal framework and infrastructure to facilitate live streaming of data sets.	Create a program structure to support the cataloging, hosting, and/or mirroring of international data sets.	Expand the educational security courses and material offered through the Defense Technology Experimental Research testbed. Expand the legal framework to support international data sharing.	Create data enclaves to support access to restricted data sets.	Expand federated capability to support non-heterogeneous resources, allowing for experiments to span from large-scale clouds to nomadic mobile devices.
Objective: Software Assurance				
Develop a systematic method to map natural language security controls to Common Weakness Enumerations.	Produce tools for identifying, analyzing, and rectifying latent vulnerabilities in software.	Pilot tools used for identifying, analyzing, and rectifying latent vulnerabilities in software.	Transition tools to commercial market and integrate into existing services.	Transition tools to commercial market and integrate into existing services.
Objective: Network Security				
Develop router traffic monitors, route tracing tools, and Internet traffic visualization tools.	Develop router traffic monitors, route tracing tools, and Internet traffic visualization tools.	Develop new tools and techniques for mapping several layers of the Internet to detect and mitigate malicious behavior.	Deliver newly developed tools that meet customer needs.	Deliver newly developed tools that meet customer needs.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Cyber Security Division (CSD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Mobile, Web, and Cloud Security				
Validate the origins of Internet routes through the operational use of the Resource Public Key Infrastructure.	Pilot near-term mobile security solutions. Pilot cloud forensics and auditing tools.	Begin testing and evaluation of an initial end-to-end secure cloud architecture. Test experimental deployment of the Border Gateway Protocol.	Assess produced cloud forensics and auditing technology approaches and solutions.	Assess the effectiveness of developed solutions to meet evolved security requirements and document gaps. Operationally deploy an end-to-end secure cloud architecture.
Objective: Identity Management and Privacy				
Conduct system integration, interoperability tests, and evaluations for federal, state, local, tribal, and territorial agencies through the Identity Management Testbed. Evaluate and award research areas through a Privacy Broad Agency Announcement.	Provide fine-grain, secure information access and physical access.	Address current federal, state, and local identity management requirements in line with ongoing federated activities through the Identity Management Testbed.	Collaborate with international entities on the global federated identity management research needs of disparate communities.	Deliver solutions for attribute-based access control while reducing identity fraud and enhancing privacy.
Objective: Cybersecurity Education and Training				
Test S&T-funded technologies in cyber gaming challenges. Transition CSIRT best practices to U.S. and international CSIRT partners.	Test S&T-funded technologies in cyber gaming challenges.	Test S&T-funded technologies in cyber gaming challenges.	Test S&T-funded technologies in cyber gaming challenges.	Test S&T-funded technologies in cyber gaming challenges.
Objective: Securing Critical Infrastructure				
Initiate Cyber Physical Systems Security research program. Establish an automotive security consortium. Complete annual R&D projects with the oil and gas subsector.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.
Objective: Transition To Practice				
Transition three technologies to the commercial market each fiscal year. Pilot three to six technologies in production environments in the HSE each fiscal year. Identify six to 10 technologies that are candidates for transition each fiscal year.				
Objective: Cybersecurity for Law Enforcement				
Test and evaluate deployable cloud forensics solutions and new capabilities in partnership with law enforcement customers.	Begin detection research, utilizing both Bayesian and machine learning approaches. Complete research and transition to DHS law enforcement components signal survey and direction-finding software.	Complete operational pilots of next-generation technology architecture for law enforcement.	Deliver updated forensic solutions for law enforcement to respond to technological advances made for personal electronic devices.	Pilot test personal electronic device research with the law enforcement community.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Explosives Division (EXD)

Vision – EXD protects citizens and our country's infrastructure against the devastating effects of explosives by seeking innovative approaches in detection and countermeasures. EXD provides concepts, science, technologies, and systems to increase the HSE's ability to detect explosives and mitigate the effects of an explosive blast. EXD will:

- Rapidly develop and deliver knowledge, analyses, and innovative solutions to counter the threat of improvised explosive devices (IEDs) against domestic targets.
- Leverage technical expertise to assist the efforts of the Transportation Security Administration (TSA) and other DHS components to establish operational requirements and select and acquire needed technologies.
- Conduct, catalyze, and survey scientific discoveries and inventions relevant to existing and emerging explosive materials and devices.

Strategic Drivers – Frequent and devastating attacks against U.S. commercial aviation and other domestic targets began in 1988 with the bombing of Pan Am Flight 103 over Lockerbie, Scotland. Threats today include attacks not just against aviation but also against mass transit (e.g., Madrid, London), fixed infrastructure (e.g., Murrah Federal Building), and public gatherings (e.g., Times Square, Boston Marathon). EXD endeavors to counter these threats by implementing the first goal of the 2014 QHSR: to prevent terrorist attacks. On September 9, 2014, the Under Secretary for Science and Technology testified before the House Committee on Homeland Security that "noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Whether screening people, baggage or cargo, unobtrusive technologies and improved processes will enable the seamless detection of threats while respecting privacy, with minimal impact to the speed of travel and the pace of commerce." More specific strategic guidance comes from the 2013 HSARPA/TSA R&D Test and Evaluation Strategic Plan, which states that S&T should endeavor to "accelerate the process of delivering new capabilities to the user that improve effectiveness and efficiency" and "support risk-driven operations to provide effective and efficient security."

Description of Capabilities:

- **Aviation Solutions** – Develop cost-effective systems for screening air cargo, checked baggage, carried items, and people at checkpoints that will improve detection capabilities, reduce false alarm rates, and improve the overall customer experience.
- **Intermodal Solutions and Facilities Protection** – Develop technologies capable of screening in high-throughput areas where traditional checkpoints are neither effective nor efficient. Enhance tools to improve current canine and trace detection screening methods.
- **Foundational Science** – Determine the explosives and blast phenomenology that makes applied R&D possible. This includes the study of explosive material characteristics relevant to discrimination and detection and the assessment of blast effects on aircraft and infrastructure.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Aviation Solutions				
Develop an air cargo screening capability for X-ray images. Conduct air cargo IED studies on six high-priority threats. Develop a checked baggage prototype with an automated target recognition algorithm. Develop a Coded Aperture X-Ray Imaging System. Integrate with current AT systems.	Study additional air cargo IED threats as part of the air cargo threat study. Modify least-risk bomb location procedures. Develop "K" and "W band" systems with auto threat detection. Develop an advanced multi-view X-ray prototype. Create a Coded Aperture Micro Mass Spectrometer Explosives Trace Detection (ETD) prototype.	Improved algorithms for checked baggage. Retrofit air cargo's ETD system. Develop Dynamic Risk Screening interfaces for checkpoint systems. Extend Advanced Imaging Technology (AIT) development for "no divestiture" screening. Develop scanning technology to extend checkpoint screening to cover liquid explosives and thin sheets.	Extend AIT development to support "walk at speed" screening. Continue development of checkpoint systems to support Tier 3 explosives and reach goal of 500 bags per hour. Work with TSA to integrate AIT and checkpoint technology with TSA concept of operations.	Transition air cargo ETD. Continue AIT development with a focus on automatic threat identification. Extend checkpoint baggage systems to support TSA goal of 600 bags per hour and detection of Tier 4 explosives.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Explosives Division (EXD)				
FY 2015	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**
Objective: Intermodal Solutions and Facilities Protection				
Evaluate Department of Defense (DOD)-sponsored standoff detection systems. Evaluate a widely tunable infrared trace source prototype. Demonstrate a person-borne standoff detection technology. Perform laboratory test and evaluation of an intelligent video algorithm with a realistic data set. Conduct operational pilots of forensic video tools providing leave-behind detection and surveillance for situational assessment.	Demonstrate vehicle eye-safe trace detection advanced feasibility. Evaluate additional widely tunable infrared trace source prototypes. Transition interim standoff trace detection capabilities from DOD. Develop an Under Rail Screening System prototype. Continue developing advanced video algorithms for leave-behind improvised explosive detection. Demonstrate system ability to detect leave-behind, replay video, associate to individual, and tag and track the individual. Deploy an intelligent video prototype.	Demonstrate and down-select a vehicle eye-safe trace detection design. Develop a layered system prototype incorporating millimeter wave imaging array. Deploy an intelligent video system in an operational environment. Conduct operational test and evaluation of the Under Rail Screening System.	Test and evaluate vehicle eye-safe trace detection prototypes. Demonstrate person-borne standoff detection advanced feasibility.	Pilot a vehicle eye-safe trace detection prototype system at federal facilities. Deploy a layered system prototype in an operational environment. Demonstrate a non-invasive Screening at Speed prototype system for standoff explosive detection in the mass transit environment.
Objective: Foundational Science				
Develop explosive safety standards. Enhance transportation security operations. Develop capabilities to characterize explosive detection signatures. Demonstrate explosive data integration.	Provide data for high-risk chemical facilities regulation. Reduce vulnerabilities by denying resources through precursor inhibition, improving detection at target locations, and enhancing data integration. Conduct a threat-informed risk analysis. Develop capabilities to characterize explosive detection signatures. Deliver component decision support tools for first responders and emergency planners regarding homemade explosives incident planning and mitigation measures.	Develop a desktop ETD prototype. Establish data sharing practices with interagency and industry partners. Develop capabilities to characterize explosive detection signatures.	Develop portable ETDs with tools and methodologies. Develop explosive detection signatures image library interface for DHS partners. Develop capabilities to characterize explosive detection signatures. Develop risk-based analysis and situational awareness tools for the DHS National Protection and Programs Directorate and the interagency.	Develop enhanced capabilities to characterize explosive detection signatures.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Resilient Systems Division (RSD)

Vision – RSD is charged with identifying and developing innovative and practical solutions to enhance the nation's resilience to all hazards.

Strategic Drivers – RSD's strategic drivers are based on national Presidential Policy Directives (PPD-8 and PPD-21), the 2014 QHSR, Federal Emergency Management Agency (FEMA) and DHS National Protection and Programs Directorate priorities, and the operational capabilities of the user community. Based on these drivers, RSD will develop innovative solutions that are readily deployable and tailored to the needs of DHS operational components and federal, state, and local users. RSD will collaborate with DHS components and other federal and international partners to reduce costs and accelerate technology transition. Similarly, RSD will strengthen existing and build new partnerships with the HSIB to transition R&D solutions into economically viable commercial products.

RSD's R&D strongly supports three department-wide strategic goals as defined in the 2014 QHSR. In support of Mission 1: Prevent Terrorism and Enhance Security, RSD's portfolio includes R&D to help prevent terrorist attacks and reduce risk to the nation's critical infrastructure, key leadership, and events. For QHSR Mission 4: Safeguard and Secure Cyberspace, RSD's projects help strengthen critical infrastructure security and resilience; cybersecurity; and law enforcement, incident response, and reporting capabilities. Finally, RSD supports QHSR Mission 5: Strengthen National Preparedness and Resilience through R&D activities aimed at enhancing national preparedness, mitigating hazards and vulnerabilities, ensuring effective emergency response, and enabling rapid recovery following an incident.

RSD conducts enabling activities in support of mission achievement, such as building and sustaining intergovernmental and public-private partnerships and facilitating outreach and information sharing to enhance community resilience and improve public awareness and preparedness. RSD also applies social and behavioral science to improve threat detection and Countering Violent Extremism (CVE) and develops innovative approaches and effective solutions to homeland security challenges.

Description of Capabilities:

- **Cyber-Physical Systems (CPS) in the Critical Infrastructure** – Transform CPS in critical infrastructure into safe, secure, and self-healing environments. Enhance the security and continuity of critical infrastructure, with special emphasis on lifeline functions and the associated interdependencies and cascading effects.
- **Disaster Response and Recovery** – Make disaster management routine, agile, and risk-informed. Increase the agility of disaster response and strengthen the capability of communities to recover rapidly from incidents and events.
- **Resilient and Risk-tolerant Communities** – Change communities into resilient and risk-tolerant organizations. Improve public preparedness, awareness, and community resilience through the integration and application of social and behavioral sciences.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: CPS in the Critical Infrastructure				
Create a CPS framework, architecture, and tool set. Create system models of cross-sector cascading effects.	Deploy a CPS framework for the electric grid; conduct field test and evaluation. Deploy system models for lifeline functions.	Extend CPS framework to communications and water; conduct field tests and evaluation. Identify and develop economic incentives for adopting resilience practices and/or technologies. Develop Wearables for Infrastructure Security and Resilience (WISER).	Transition and deploy a CPS framework in the energy and power sector. Pilot economic incentives for resilience in communities. Develop and refine WISER.	Transition to multiple sectors and conduct field exercises. Deploy WISER.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Resilient Systems Division (RSD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Disaster Response and Recovery				
Create a system-of-systems decision support tool to enhance flood response and recovery. Modernize the National Hurricane Program (NHP) to speed evacuation planning.	Develop community rating metrics for the National Preparedness and Response programs. Deploy risk-based modeling and simulation tools for natural hazards planning.	Develop fusion algorithms for flood management. Develop fusion algorithms and an evacuation decision tree model for FEMA regions.	Integrate data sets for the National Preparedness and Response programs and conduct operational field tests and evaluation. Integrate models and data for NHP and start transition to FEMA operations.	Conduct field testing on the Relational Adaptive Processing of Information and Display Apex program. Deploy updated NHP system within FEMA and state and local regions.
Objective: Resilient and Risk-tolerant Communities				
Establish an international community for CVE. Transition the Terrorism and Extremist Violence in the United States (TEVUS) database. Start CVE engagements with Australia, Israel, and the United Kingdom.	Develop a CVE strategy. Build a knowledge repository on CVE trends, indicators, and lessons learned. Research social and behavioral factors related to public messaging and CVE activities.	Execute further research to understand, identify, and divert violent extremism. Build community cohesion and communicate a counter narrative. Continue social and behavioral research related to public messaging and CVE activities.	Scale and expand CVE engagement with Five Eyes nations. Apply results of social and behavioral research to improve the effectiveness of public messaging and government CVE activities.	Deploy CVE products for the law enforcement community, fusion centers, and other federal agencies.

FIRST RESPONDERS GROUP DIVISIONS

First Responder Technologies (R-Tech)

Vision – First responders will have the force multiplying tools and solutions that allow them to save lives and maximize preparedness.

Strategic Drivers – A major strategic driver is consistency with department-wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Additionally, R-Tech's strategic priorities are driven by the needs of first responders who want more situational awareness and protection when they approach an incident.

Description of Capabilities:

- **Personal Protective Equipment (PPE) and Tools** – Develop advanced PPE and tools for first responders to protect lives, increase their safety, and mitigate damage.
- **3-D Location and Response Awareness** – Deliver geo-location integrated technologies that track first responders, threats, and resources available to support response operations.
- **Technology Clearinghouse** – Provide a first responder technology clearinghouse that enhances technical information exchanges, delivers advanced training tools, and ensures the validity of software.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: PPE and Tools				
Develop Phase II Multi-Threat Textile to provide first responders with enhanced protection from stabbing, fire, biological, and other hazards. Conduct performance testing on prototype materials and write report.	Develop a Thermal Imaging Camera that can be integrated into a self-contained breathing apparatus (SCBA) to provide first responders with enhanced on-scene imagery while fighting fires. Conduct an operational field assessment of the thermal imaging camera and write report.	Commercialize Finding Individuals for Disaster and Emergency Response (FINDER) tool, which provides urban search and rescue teams with the ability to detect human heartbeats in rubble or buildings during a disaster.	Develop tools to increase exposure detection of unknown threats such as toxins, biological agents, or contaminants during response operations. Conduct an operational field assessment of detection tools.	Create self-decontaminating PPE to provide protection against biological agents, by providing an effective barrier to bacteria, which is innocuous to the human wearer and is lightweight and breathable. Conduct performance testing on PPE and write report.
Objective: 3-D Location and Response Awareness				
Commercialize Improved Structure Firefighting Glove to provide on-scene firefighters with enhanced dexterity and donn/doff-ability.	Develop enhanced mobile biometrics, to provide on-scene first responders with iris, face, and fingerprint readers to assist them in obtaining accurate near real-time identifications. Conduct an operational field assessment of mobile biometric tools.	Develop Lost Person Locator Tool for first responders to use when searching for lost individuals. Publish guidance, protocols, and strategies for the lost person locator tool.	Develop a system to detect, monitor, and analyze passive and active threats and hazards at incident scenes. Conduct an operational field assessment of above system.	Develop persistent surveillance tools to enhance a first responder's awareness of on-scene threats and hazards. Conduct an operational field assessment of persistent surveillance tools and write report.
Objective: Technology Clearinghouse				
Begin transition of the Virtual Training module, to provide first responders with realistic training scenarios that enhance their skills and confidence to respond effectively and efficiently during real-life incidents.	Finalize transition of the Virtual Training module to the first responder community.	Upgrade First Responder Support Tools (FiRST) app to include enhanced situational awareness of explosive threats.		

FIRST RESPONDERS GROUP DIVISIONS CONTINUED

Office for Interoperability and Compatibility (OIC)

Vision – First responders and the public will always have the emergency preparedness, mitigation, response, and recovery information they need.

Strategic Drivers – A major strategic driver is consistency with department-wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, OIC's strategic priorities are consistent with the One DHS Executive Committee Strategy Goal 1: Integrate and enhance emergency communications capabilities through common enterprise architecture. Additionally, OIC's strategic priorities are driven by the needs of first responders who seek interoperability and compatibility research, development, testing, and evaluation expertise that focuses on bridging land mobile radio (LMR) and broadband networks and improving LMR network efficiency.

Description of Capabilities:

- **Voice and Data Communications** – Empower first responders to talk to each other and share data without worrying about underlying technology.
- **Information Sharing** – Enable first responders to securely exchange useful, actionable information in time to make a difference.
- **Alerts, Warnings, and Notifications (AWN)** – Articulate a rational, integrated approach to AWN for all hazards and all threats.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Voice and Data Communications				
Develop capabilities for LMR–Long Term Evolution (LTE) interoperability. Develop concepts for a First Responder Personal Area Network (PAN). Develop a business process model to establish baseline costs of Project 25 (P25) performance, conformance, and interoperability testing.	Establish a 700 MHz demo network. Transition LMR–LTE interoperability capabilities to first responders. Develop and test the initial architecture of the First Responder PAN. Support public safety broadband (FirstNet) architecture development. Establish testing capabilities to determine LMR conformance with the P25 suite of standards.	Conduct security research and testing of 700 MHz network and LMR–LTE interoperability. Integrate the First Responder PAN technology with LMR and LTE. Support FirstNet architecture development. Transition the First Responder PAN technology for operational use. Initiate a P25 conformance testing program.	Add on capabilities for LMR, including audio and video quality tools. Conduct P25 testing. Support FirstNet architecture development. Conduct P25 testing.	Release the Video Quality in Public Safety Handbook v3. Conduct P25 testing. Support FirstNet architecture development.
Objective: Information Sharing				
Standardize computer-aided dispatch (CAD) and mutual aid information sharing. Transition first responder collaboration tools.	Transition CAD and mutual aid standardization tools. Design architectural concepts for the public safety cloud (PSC), including identity and access management (IdAM) requirements.	Develop PSC standards and demo projects. Conduct IdAM application demonstrations, including a Backend Attribute Exchange Pilot. Conduct an Internet of Things demonstration.	Transition PSC technologies for operational use. Develop next-generation 911 standards. Develop standards for Internet of Things use by first responders.	Develop and transition technologies to allow first responders to securely exchange information as needed.
Objective: Alerts, Warnings, and Notifications				
Conduct Wireless Emergency Alerts webinars. Develop a public AWN architecture.	Release the Emergency Data Exchange Language Common Alerting Protocol Report.	Develop geo-targeted AWN. Define the next-generation 911 interface.	Develop approaches and standards for citizen-to-government AWN.	Demonstrate citizen-to-government AWN, including next-generation 911 and other methods.

FIRST RESPONDERS GROUP DIVISIONS CONTINUED

National Urban Security Technology Laboratory (NUSTL)

Vision – First responders will have the test, evaluation, and assessment services and radiological nuclear response recovery tools they need.

Strategic Drivers – A major strategic driver is consistency with larger department-wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Additionally, NUSTL's strategic priorities are driven by the needs of first responders who want to understand and inform the development of emerging technologies for the public safety community in various operational field environments.

Description of Capabilities:

- **Tests, Evaluations, and Assessments** – Ensure effectiveness, performance, and suitability of technologies for operational deployment.
- **Technical Advisors to First Responders** – Bridge the knowledge gap between technology developers and end users.
- **Radiological Nuclear Response and Recovery** – Save lives, minimize economic impact, and enhance resiliency following a radiological or nuclear event.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Tests, Evaluations, and Assessments				
Conduct NUSTL Urban Operational Experimentation.	Improve the impact of the System Assessment and Validation for Emergency Responders program.	Test first responder technologies for HSARPA divisions.	Conduct SAFETY Act validation and verification testing.	Serve as a FEMA grant acquisition and quality assurance test agent.
Objective: Technical Advisors to First Responders				
Host the New York Area Science and Technology Forum.	Provide training and exercise support to first responders.	Upgrade the Sensitive Compartmented Information Facility.	Develop standards for first responder technologies.	Develop and lead alliance of laboratories supporting first responders.
Objective: Radiological Nuclear Response and Recovery				
Establish improvised nuclear device decision making skill requirements.	Develop science-based tactical response guidance for a Radiological Dispersion Device.	Research disaster-resilient communications and post-event messaging.	Develop tools for decision making based on radiological data. Develop guidelines for radiological operational support specialist positions under the National Incident Management System.	Provide emergency dosimetry guidance for radiological emergencies.

APEX PROGRAMS

Apex Program – Air Entry/Exit Re-engineering (AEER)

Vision – The Apex AEER program will transform immigrations and customs inspections of international air travelers traveling through the busiest U.S. international airports. The program is a collaborative effort between CBP and a multi-disciplinary team from S&T to analyze existing CBP Office of Field Operations processes and identify, develop, test, and evaluate new concepts of operations and approaches to enhance and facilitate traveler screening processes. The program will also develop recommended approaches and technologies to provide CBP with cost-effective and integrated biometric entry and exit capabilities. With these solutions, CBP will be able to increase its ability to confirm the identity of persons entering and departing the United States; fulfill its obligation to implement a biometric air exit solution mandated by Congress; and ensure that processes are efficient and continue to facilitate international travel, tourism, and economic growth.

Strategic Drivers – CBP is responsible for enforcing U.S. immigration and customs laws, while also facilitating international trade and travel beneficial to our economy. Increases in international air travel are straining CBP resources, resulting in increased wait times and delays for passengers to clear Federal Inspection Service areas. Additionally, DHS is statutorily required by 8 U.S.C. 1365b(d) to provide biometric entry and exit data and by 8 U.S.C. 1187(i), which requires an exit system that matches biometric information of foreign travelers against relevant watch lists and immigration information. Furthermore, the Presidential National Travel and Tourism Strategy requires DHS to take additional steps to expedite the entry process and reduce wait times for travelers. There are three primary drivers for AEER: a) facilitate trade and travel; b) implement new and improved operational capabilities required by federal legislation; and c) support the Presidential National Travel and Tourism Strategy.

Description of Capabilities:

- **Maryland Test Facility and Scenario-based Testing** – Provides a low-cost, adaptive, and configurable controlled environment for laboratory and scenario-based testing to evaluate biometric technologies, processes, and concepts of operation under realistic, simulated airport entry and exit conditions.
- **Business Case Analysis** – Assess proposed biometric and non-biometric solutions and select those that are deemed most suitable for an operational field trial. Develop a Business Case Analysis that contains cost estimates, such as infrastructure enhancements, staffing, and technology to inform potential CBP business process transformation, system development, and technology acquisition.
- **Operational Field Trial** – Conduct a field trial at an air POE to determine the performance of a complete biometric exit system under real-world conditions.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Maryland Test Facility and Scenario-based Testing				
Complete scenario-based test and evaluation. Transition entry business transformation initiatives to CBP.	Support preparations for a field trial in an operational setting. Transition entry business transformation initiative to CBP.	(Apex AEER ends in FY 2016)		
Objective: Business Case Analysis				
Deliver biometric exit business case analysis inputs.	Deliver a Business Case Analysis to CBP for acquisition follow-up and development of draft acquisition documentation.			
Objective: Operational Field Trial				
Select airport site candidates for field evaluation; select biometric technology candidates for field evaluation.	Initiate and complete field trial evaluation. Transition exit field trial system technical specifications to CBP.			

APEX PROGRAMS CONTINUED

Apex Program – Border Enforcement Analytics Program (BEAP)

Vision – BEAP combines emerging data analytics capabilities with ICE senior agent knowledge to create data-driven methodologies that directly support key goals for the Administration's Export Control Reform initiatives, counter-proliferation efforts led by ICE's Homeland Security Investigations (HSI), and the interagency Export Enforcement Coordination Center (E2C2). The program flattens access to relevant data sources and makes tools available that enable rapid access to information used in enforcement actions. Using the BEAP model for counter-proliferation investigation support, S&T is translating capabilities to additional relevant investigation domains within HSI.

Strategic Drivers – There are three primary drivers for BEAP: a) improving export controls for critical commodities and technologies; b) Presidential Executive Order 13558, which established E2C2; and c) United Nations Security Council Resolution 1540 regarding non-proliferation controls for materials related to weapons of mass destruction. ICE HSI leads E2C2 and maintains unique authorities to access data sources related to export enforcement.

Description of Capabilities:

- **Exploratory Methods Mapping (EMM)** – Record knowledge from retired ICE agents with more than 30 years of experience in order to identify methods and algorithms that can identify illicit activity in data sets.
- **S&T Enclave (STE)** – Create an exploratory laboratory where technical capabilities are mapped to agent-created methods and algorithms. Conduct performance assessments to improve the computation and accuracy of results.
- **Big Data Environment (BDE)** – Deploy development operations and operations support systems to integrate successful algorithms that are successful in the S&T environment.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Exploratory Methods Mapping				
Demonstrate new algorithms to ICE leadership and Special Agent in Charge offices. Transition three key algorithms to BDE to support HSI and E2C2 operations.	Transition EMM operations to ICE HSI and E2C2.	(Apex BEAP ends in FY 2016)		
Objective: S&T Enclave				
Complete studies of Internet Protocol geocoding and entity resolution for ICE. Transition geo-coding and entity resolution results to BDE.	Transition STE operations to the HSARPA Data Analytics Engine portfolio.			
Objective: Big Data Environment				
Complete the transition and integration of BDE to ICE HSI operations. Fully implement support for additional investigation domains.	Transition BDE operations to ICE HSI, Chief Information Officer, and E2C2.			

APEX PROGRAMS CONTINUED

Apex Program – Border Situational Awareness (BSA)

Vision – CBP and partner law enforcement agencies at the federal, state, local, tribal, and international levels need improved situational awareness to more effectively and efficiently deploy resources to the areas of highest risk, particularly along land borders on the U.S. Southwest border. The Apex BSA program will enable the HSE to increase border situational awareness, leading to increased border incursion detection, interdictions, and deterrence. The Apex BSA program will improve border situational awareness by establishing an enterprise capability to a) access more data sources; b) make available decision support tools to translate available data into actionable information and intelligence; and c) share that actionable information and intelligence with partner law enforcement agencies.

Strategic Drivers – BSA's future efforts will be guided by 2014 QHSR Mission 2: Secure and Manage our Borders (specifically goals 2.1 and 2.3), 2014 QHSR Mission 3: Enforce and Administer our Immigration Laws (specifically goal 3.2), and S&T's Visionary Goal "Enable the Decision Maker: Actionable Information at the Speed of Thought." BSA's efforts will also be influenced by the 2014 QHSR's strategic aim to Mature and Strengthen Homeland Security by focusing on (1) integrating intelligence, information sharing, and operations; (2) enhancing partnerships and outreach; and (3) conducting homeland security R&D. BSA will derive much of its requirements from the DHS Campaign Plan for Securing the U.S. Southern Border and Approaches (Jan 23, 2015). In addition, the execution of BSA's research will focus on (1) operations, innovation, and partnerships, specifically by transitioning mature and rapidly deployable solutions to DHS operational components; (2) developing technologies that have a positive impact on operations and return on investment for our customers; (3) collaborating with DHS components, other government agencies, and international partners to reduce R&D, operation, and maintenance costs, as well as time to delivery; and (4) partnering with industry to transition new technologies and guide their investments.

Description of Capabilities:

- **Enterprise Information Sharing Architecture** – Build the system architecture; leverage existing Intelligence Community, DOD, and DHS investments. Ingest existing data sources currently in operational use. Integrate existing cost-effective decision support tools (e.g., analysis, fusion, visualization).
- **Tactical Decision Support and Mobile Communications Solutions** – Focus on border patrol station-level tactical use cases defined through field stakeholder workshops. Integrate technologies for low bandwidth/mobile users (e.g., tactical technologies). Integrate emerging decision support tools to inform tactical-level decisions.
- **Strategic Planning and Resource Decision Support Solutions** – Focus on DHS use cases defined through stakeholder workshops. Integrate risk assessment tools to inform manpower and equipment resource allocation. Integrate strategic planning and resource decision support tools as needed.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Enterprise Information Sharing Architecture				
Initiate the program and obtain ESC approval. Perform requirements analysis of Enterprise Information Sharing Architecture capability.	Develop Enterprise Information Sharing Architecture capability.	Pilot, validate, and transition Enterprise Information Sharing Architecture capability.		
Objective: Tactical Decision Support and Mobile Communications Solutions				
		Perform requirements analysis and initiate development of Tactical Decision Support and Mobile Communications Solutions capability.	Develop, pilot, and validate Tactical Decision Support and Mobile Communications Solutions capability.	Transition Tactical Decision Support and Mobile Communications Solutions capability.
Objective: Strategic Planning and Resource Decision Support Solutions				
			Perform requirements analysis of Strategic Planning and Resource Decision Support Solutions capability.	Develop Strategic Planning and Resource Decision Support Solutions capability.

APEX PROGRAMS CONTINUED

Apex Program – Relational, Adaptive Processing of Information and Display (RAPID)

Vision – This Apex program will make communities more resilient to disruptive events through the creation and application of a decision support system-of-systems for community risk assessment and resilience planning. This program aims to save lives, reduce property losses, and enhance overall resilience. The flood hazard is the first use case.

Strategic Drivers – A major strategic driver is consistency with larger department-wide strategic frameworks, including the goals under 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, FEMA and partner communities (state, local, tribal, territorial) need better quality data and improved awareness to more effectively respond to and plan for flood events in support of FEMA Strategic Priority 4: Enable Disaster Reduction Naturally.

The RAPID Apex program supports implementation of Presidential Policy Directives 8 and 21—National Preparedness, and Critical Infrastructure Security and Resilience, respectively—as well as FEMA's Federal Flood Risk Management Standard and Executive Order 13690, Establishing a Federal Flood Risk Management Standard and a Process for Further Soliciting and Considering Stakeholder Input. The RAPID Apex program directly links to S&T's Visionary Goals, which were informed and validated by the stakeholder community.

Description of Capabilities:

- **Community Rating System Demonstration Study** – Identify indicators of resilience in National Flood Insurance Program communities participating in the Community Rating System (CRS).
- **Data Roadmap** – Create a data roadmap identifying critical data sources sufficient to support resilience indicators and all emergency support functions.
- **Community Performance Benchmarking** – (a) Conduct pilot studies in six CRS communities with historic flood performance data; (b) validate resilience indicators from a CRS demo study; and (c) identify any new resilience indicators.
- **Community Pilots** – Conduct three regional pilots to determine the effectiveness of the resilience indicators across scales (e.g., mutual aid).
- **Technology Portfolio** – (a) Study the impact of technology solutions on communities and generate cost/benefit metrics and (b) quantify three to five critical technology solutions for each critical infrastructure lifeline function for low-, medium-, and high-risk/cost tolerances by FEMA region.
- **Decision Support Logic** – (a) Create algorithms to support common decision support needs; (b) create backend interfaces with algorithms, data sets, and analytics; and (c) create a user interface.
- **Transition to Use** – Field test applications in three to five events and exercises in two FEMA regions. Iterate development of the user interface based on feedback.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Community Rating System Demonstration Study				
Identify indicators of resilience in communities participating in the National Flood Insurance Program's CRS.	....	....	....	....
Objective: Data Roadmap				
Create a data roadmap identifying critical data sources sufficient to support resilience indicators and all emergency support functions.	....	....	....	....

APEX PROGRAMS CONTINUED

Apex Program – Relational, Adaptive Processing of Information and Display (RAPID)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Community Performance Benchmarking				
	Conduct pilot studies in six CRS communities with historic flood performance data. Validate resilience indicators from a CRS demo study. Identify any new resilience indicators.			
Objective: Community Pilots				
	Conduct three regional pilots to determine the effectiveness of the resilience indicators across scales (e.g., mutual aid).	Continue regional pilots.		
Objective: Technology Portfolio				
	Study the impact of technology solutions on communities and generate cost/benefit metrics.	Quantify three to five critical technology solutions for each critical infrastructure lifeline function for low-, medium-, and high-risk/cost tolerances by FEMA region.		
Objective: Decision Support Logic				
	Create algorithms to support common decision support needs. Create backend interfaces with algorithms, data sets, and analytics. Create a user interface.			
Objective: Transition to Use				
				Field test applications in three to five events and exercises in two FEMA regions. Iterate development of the user interface based on feedback.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation Cyber Infrastructure

Vision – S&T partners with the Financial Services Sector to develop and deliver advanced sensing technologies, situational understanding, response and recovery, and network protections to the institutional, sector, and cross-sector levels.

Strategic Drivers – The S&T Visionary Goal "A Trusted Cyber Future: Protecting Privacy, Commerce, and Community" and the 2014 QHSR goals 4.3 and 4.4 will guide CSD's research in the years to come. CSD will aim to improve the underlying infrastructure of the digital world and ensure information is protected, illegal use of information is deterred, and privacy is not compromised. Primary technological and threat drivers include:

- The continued growth of the Internet of Things, which will result in heretofore unconnected devices interacting via the Internet
- The interconnection of multiple aspects of life (e.g., critical infrastructure, medical devices, automobiles) that depend on digital devices and information. As this continues to expand, the impacts and consequences of these connections will become increasingly difficult to predict.
- The barriers to entry for cyber criminals, "hacktivists," and cyber terrorists will decrease, expanding the pool of those who can disrupt the cyber infrastructure.

Policy directives and implementation will also continue to impact CSD's research portfolio. Recent legislation and executive orders have, for example, established requirements for a National CISR R&D plan, launched a National Cyber Threat Intelligence Integration Center, and called for a Federal Cybersecurity R&D plan (Cybersecurity Enhancement Act of 2014). Policy, however, will continue to lag behind technology advances, thus creating seams or gaps in the regulation and enforcement of cybersecurity norms and development of technical solutions.

Description of Capabilities:

- **Advanced Sensing Technologies** – Improve measurement and attestation to reveal the presence or absence of attacker modifications to network infrastructure and model network behavior.
- **Situational Understanding** – Develop sensor correlation capabilities (alerts and human inputs) to present relevant observations of human understanding and the capability to characterize the underlying digital infrastructure from the routing to network layers.
- **Response and Recovery** – Develop the capability to execute rapid, policy-based, and situation-specific responses, including but not limited to reconfiguring sensor grids to clarify a situation, reconfiguring systems and networks to maintain operationally critical services, and returning a network to its last known valid and secure state.
- **Network Protection** – Advance network control planes, including but not limited to secure routing for Distributed Denial Of Service protection, secure route origination and end-to-end routing, secure dynamic enclaves, on-demand asset control to maintain network essential services, and secure browsing.
- **Operational Exercises** – Deliver the capability and capacity to run realistic exercises from the institutional level up to sector-wide.
- **Common Messaging and Interfaces** – Develop or leverage common message traffic protocols to improve information sharing, including cyber threat indicators.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Advanced Sensing Technologies				
Expand current insider threat body of knowledge and initiate improved measurement mechanisms research.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.
Objective: Situational Understanding				
Characterize networks based on passive traffic analysis and other attributes.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.
Objective: Response and Recovery				
Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation Cyber Infrastructure				
FY 2015	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**
Objective: Network Protection				
Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.
Objective: Operational Exercises				
Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.
Objective: Common Messaging and Interfaces				
Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation First Responder (NGFR)

Vision – The NGFR Apex program envisions a responder of the future who is protected, connected, and fully aware. Armed with comprehensive physical protection, interoperable tools, and networked threat detection and mitigation capabilities, cross-functional responders of the future will be better able to serve their communities. The NGFR Apex program will integrate existing and emerging communications technologies and sensors into responders' protective garments and standard equipment, making each responder a mobile, wireless communications hub and sensor platform linked automatically to a wide-ranging mesh network.

Strategic Drivers – A major strategic driver is consistency with larger department-wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, the NGFR Apex program is consistent with the One DHS Executive Committee Strategy Goal 1: Integrate and enhance emergency communications capabilities through common enterprise architecture. Moreover, the NGFR Apex program is directly linked to S&T's Visionary Goals, which were informed and validated by the stakeholder community.

Description of Capabilities:

- **Real-time Situational Awareness** – Develop game-changing tools for wearable, interoperable communications systems; indoor tracking of first responders; and incorporation of information from multiple and nontraditional sources (e.g., crowdsourcing, social media) into incident command and operations.
- **Duty Uniforms and PPE** – Provide detection, monitoring, and analysis of passive and active threats and hazards at incident scenes in real time.
- **Responder Technology Alliance** – Harness the HSIB and venture capital to enable collaborative commercialization of technologies.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Real-time Situational Awareness				
Develop baseline requirements, assess technologies, define an architecture, and build a technology roadmap.	Demonstrate wearable technology, Mobile Ad Hoc Networking, and Long Term Evolution prototype.	Provide tools for real-time tracking of incidents and units. Enhance pre-loading of data.	Develop a fully aware hands-free display that provides dynamic data and is voice-activated.	Demonstrate full, two-way data sharing between first responder agencies and practitioners.
Objective: Duty Uniforms and Personal Protective Equipment (PPE)				
Define performance criteria and identify operational, testing, and evaluation requirements for duty uniforms and PPE.	Produce 150 "America's Missing: Broadcast Emergency Response" prototype garment ensembles for DHS.	Conduct extended operational field assessments and down-select prototypes.	Conduct wearable technology pilots.	Conduct wearable technology pilots.
Objective: Responder Technology Alliance				
Develop Responder of the Future: Industrial Visionary Design.	Develop systems-engineered solution management plans and launch responder technology accelerators.	Develop responder of the future enterprise technologies to link responders and operation centers.	Achieve commercialization and supply chain acceptance of responder technology through responders, industry, the investment community, and R&D organizations.	Achieve commercialization and supply chain acceptance of responder technology through responders, industry, the investment community, and R&D organizations.

APEX PROGRAMS CONTINUED

Apex Program – Real-time Biothreat Awareness

Vision – The Real-time Biothreat Awareness Apex program aims to minimize the consequences from the release of chemical and biological agents. The program will reduce the time it takes for decision makers to take action. This will be accomplished through improved situational awareness of a bio-event; consistent messaging across federal, state, and local stakeholders resulting in effective response guidance; and efficient recovery of infrastructure to normal use.

Strategic Drivers – CBD's Apex core requirements draw from multiple national policy documents including: National Biosurveillance Science and Technology Roadmap (2013), National Strategy for BioSurveillance (2012), 2014 QHSR, and National Biosurveillance Integrated Center Strategic Plan on Biosurveillance (2012).

The primary technology and threat drivers include:

- Threat agents are more accessible than ever, and the proliferation of technology has made it easier for non-state actors to enhance existing pathogens, or engineer new pathogens allowing them to remain undetected by traditional detection methods.
- Readiness and preparedness requires early identification of significant health incidents involving naturally occurring, accidental, or man-made threats to inform and alert decision makers.
- Well-informed decisions require the integration of contextual information derived from multiple data sources from public health networks and environmental sensors in nearly real time.
- Current capabilities in the U.S. government do not aggregate data and inform decision makers in a timely manner.

Description of Capabilities:

- **Requirements** – Determine the information needed to affect a response; develop environmental sensors that detect bio-threats at levels relevant for public health that differentiate near neighbor bio-agents; demonstrate technology triggers that inform short-term actions that include rapid confirmatory testing; evaluate bio-threat detection capability orthogonal to PCR; identify the contextual data needed to inform decision makers in order to appropriately address the desired response.
- **Integration** – Implement interconnected sensor and data networks to collect data needed to inform a response through contextualization of the bio-event.
- **Analytics** – Exploit interconnected networks for biosurveillance; develop near real-time data analysis and visualization to inform decision makers; transform the data to knowledge that informs decision making.
- **Demonstrations** – Show reduced time to inform responses by decision makers.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Requirements				
Select sites for joint operational demonstrations and exercises with DOD to inform data needs.	Complete a biosurveillance technologies assessment. Complete a tailored risk assessment for biosurveillance activities. Determine the decision makers' biosurveillance information needs.	Complete a requirements assessment based on operational testing and end users' best practices.		
Objective: Integration				
Deliver an architecture framework for a national biosurveillance system that integrates government and commercial networks.	Deliver a prototype architecture capable of fusing three to four data modalities for anomaly detection.	Evaluate alternative data sources (e.g., Internet of Things, social media, diagnostics).		
Objective: Analytics				
	Complete a study on uncertainty propagation in decision trees.	Demonstrate decision uncertainties and certainties using compiled data sets.	Transition data aggregation and visualization tools to end users.	
Objective: Demonstrations				
	Demonstrate enhanced environmental detection technologies.	Complete a laboratory demonstration of dual-use sensor concepts for environmental threat detection. Complete a large-scale demonstration of environmental sensor systems to evaluate their performance.	Complete an information fusion exercise for discerning and understanding two simultaneous unknown threats.	

APEX PROGRAMS CONTINUED

Apex Program – Screening at Speed

Vision – The aviation checkpoint of the future will efficiently detect threats to aviation security while minimizing inconveniences to passengers. Passengers will approach the checkpoint and be identified (eventually through biometrics) and assigned a risk level. The passenger will place their carry-on items on a conveyer belt leading to an enhanced X-ray device with automatic threat recognition software. The passenger will then walk through a screening portal with minimal divesture of carried items. The systems will be dynamically configured according to the passenger's risk level. A very small number of passengers will be diverted to secondary inspection where non-invasive techniques will be used to resolve alarms from the carry-on inspection system or the screening portal. Transportation security officers at the checkpoint will spend less time searching complicated two-dimensional images and more time observing and assisting passengers and resolving alarms identified by the automatic threat recognition software. In short, the Screening at Speed Apex program will enhance security, enhance efficiency, and improve passengers' experience.

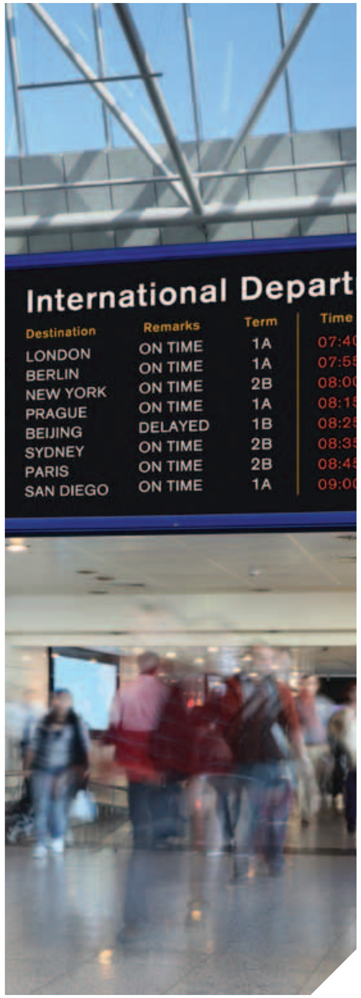
Strategic Drivers – Frequent and devastating attacks against U.S. commercial aviation and other domestic targets began in 1988 with the bombing of Pan Am Flight 103 over Lockerbie, Scotland. Since then, there have been at least 10 attempts to destroy aircraft with IEDs, five of which targeted U.S. aircraft or U.S.-bound aircraft. All but one of these five plans called for suicide bombers to smuggle IEDs through an aviation checkpoint. On September 9, 2014, the Under Secretary for Science and Technology testified before the House Committee on Homeland Security that "noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Whether screening people, baggage or cargo, unobtrusive technologies and improved processes will enable the seamless detection of threats while respecting privacy, with minimal impact to the speed of travel and the pace of commerce." More specific strategic guidance comes from the 2013 HSARPA/TSA R&D Test and Evaluation Strategic Plan, which states that S&T should endeavor to "accelerate the process of delivering new capabilities to the user that improve effectiveness and efficiency" and "support risk-driven operations to provide effective and efficient security."

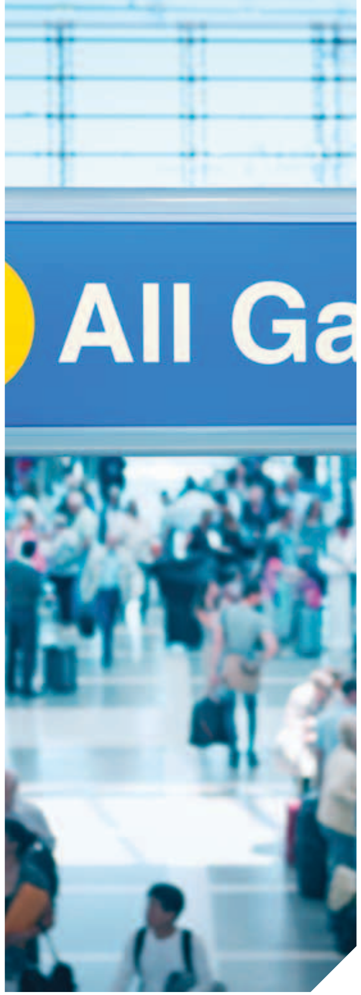
Description of Capabilities:

- **Carry-on Bag Screening** – Develop enhanced Advanced Technology (AT/AT2) carry-on bag screening systems with automatic threat recognition (ATR) capability. Develop new more capable carry-on bag screening technologies capable of three dimensional imaging and improved material discrimination.
- **Passenger Screening** – Enhance Advanced Imaging Technology (AIT) passenger screening capabilities to minimize divesture and remove the need to "stop and pose."
- **Secondary Screening** – Enhance secondary screening processes and technologies to detect a broader range of threats with greater certainty and a low false alarm rate.
- **Application Program Interfaces** – Design a set of application program interfaces for checkpoint screening systems that enable implementation of TSA's risk-based screening programs.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Carry-on Bag Screening				
Conduct test and evaluation of a carry-on bag screening system with 3-D imaging.	Develop an advanced "AT2" X-ray prototype.	Enhance multi-energy X-ray systems.	Develop X-ray systems with dynamically configurable detection thresholds.	Demonstrate a prototype with fully functional automatic threat detection software.
Objective: Passenger Screening				
Demonstrate the AIT K-band with dynamic aperture and automatic threat detection.	Integrate "K" and "W" systems with auto threat detection.			Demonstrate walk-through of an AIT prototype with automatic threat detection software.
Objective: Secondary Screening				
Demonstrate an electronic device scanning system.	Develop a coded aperture micro mass spectrometer (ETD) prototype.	Develop more efficient sampling techniques for explosive trace detection.	Release an enhanced trace library.	Develop a prototype for a non-contact ETD system.
Objective: Application Program Interfaces				
	Draft application program interface requirements.	Demonstrate Security Technology Integrated Program (STIP)-compliant primary and secondary screening products.		Demonstrate a fully integrated checkpoint that can respond to external risk input.

APEX PROGRAMS CONTINUED





TECHNOLOGY ENGINES

Technology Engines

Vision – Technology Engines are centralized functions that will provide standardized services to all Apex projects and across S&T. They will tailor their work based on each Apex program's individual focus, as well as requirements and future concepts. Through input from S&T subject matter experts and technology developers, the Technology Engines will provide best practices, technical services, expertise, lessons learned, reusable products, and solutions for Apex programs and other projects and initiatives.

Strategic Drivers – S&T's five visionary goals coalesced both in the expanded Apex program and the stand-up of the Technology Engines, which augment S&T core capabilities through the provision of cross-cutting capabilities; identification of near-term technology solutions developed by external partners, including non-traditional performers; and delivery of program and technology analysis, knowledge products, and recommendations on the future of technological innovation.

Description of Capabilities:

- **Situational Awareness and Decision Support (SANDS)** – Establish standards, specifications, capabilities, and best practices that allow secure, compatible, and relevant information sharing across the HSE and assured, secure access to databases, knowledge bases, modeling and simulation tools, and shared situational awareness products.
- **Communication and Network Technologies (CNET)** – Provide Apex programs with integrated communications and networking solutions that ensure operability and interoperability across all network platforms, ensuring the efficient and effective exchange of voice, video, and data information.
- **Data Analytics (Big Data)** – Enable Apex programs to leverage emerging storage, security, computation, and analytics technologies to create information analysis and sharing capabilities and rapidly convert data to decisions for homeland security systems, missions, and operations.

Four additional Technology Engines are emerging as "start-ups" for FY 2015: Human Systems, Identity Access and Management, Modeling and Simulation, and Manufacturing.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: SANDS – Geospatial Analytics and Processing; Open Data Standards and Exchange; Information Sharing and Integration; System Architecture Interoperability Visualization; Decision Support Services; Interoperable Voice and Data Communications				
Stand up a fully functioning and integrated SANDS Engine. Define Apex SANDS decision support requirements for: 1) Real-time Biothreat Awareness 2) Border Situational Awareness System Architecture Interoperability Visualization: 1) Perform BSA SOA Awareness	Geospatial Analytics, Processing, and Visualization: 1) Identify operational and functional capabilities. 2) Assess satellite data availability tool. Open Data Standards and Exchange: Assess open standards for data and sensors. Information Sharing and Integration: Coordinate with the information sharing community for independent validation and verification of requirements and capabilities. System Architecture Interoperability Visualization: Determine Apex BSA enterprise integration requirements. Decision Support Services: Develop mutual aid resource access capabilities.	Define SANDS requirements for emerging Apex priorities.		

TECHNOLOGY ENGINES CONTINUED

Technology Engines

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: CNET – Interoperable Voice and Data Communications; Indoor Location and Communications; Public Safety Broadband Video Quality Applications and Services; Audio Quality for Public Safety; Land Mobile Radio Standards and Compliance; Wireless Infrastructure Modeling				
Stand up a fully functioning and integrated CNET Engine.	Interoperable Voice and Data Communications: Integrate LMR, commercial LTE networks, and the Nationwide Public Safety Broadband Network. Indoor Location and Communications: Develop a wearable heads-up display with enhanced reality. Public Safety Broadband Video Quality Applications and Services: Develop accelerated quality platforms supporting large-volume video applications. P25 Standards and Compliance: Deliver assessment program maximizing radio interoperability. Wireless Infrastructure Modeling: Guide utilization of public safety wireless.	Define CNET requirements for emerging Apex priorities.		
Objective: Data Analytics – S&T Data Analytics Lab; Exploratory Methodology Mapping (EMM); Rapid Experimentation, Prototypes and Pilots (Rapid); Assessment of Emerging Technologies (Emerging); Strategic Research and Development Engagement (Strategic)				
Server Multi-tenant, on-site facility EMM: Counter-proliferation, cyber crimes Rapid: Streaming data sets, Internet Protocol geocoding, entity resolution Emerging: Graph architectures, spark Strategic: Office of Science and Technology Policy, Berkeley AMPlab (Algorithms, Machines and People)	Server Multi-tenant, on-site facility EMM: Counter-proliferation, cyber crimes Rapid: Streaming data sets, Internet Protocol geocoding, entity resolution Emerging: Graph architectures, spark Strategic: Office of Science and Technology Policy, Berkeley AMPlab (Algorithms, Machines and People)	EMM: Cyber analysts, biothreat assessment Rapid: Large-scale sensor streams, instrumenting the analyst Emerging: Personal assistants Strategic: International collaboration	Scale Single Memory Model, transition of lab operations to the gov-cloud EMM: Disaster response in instrumented environments Rapid: Lambda architecture for targeting Emerging: Instrumented Environments and Objects	Mobile Distributed File System, hybrid commercial, gov-cloud EMM: Cybersecurity analysis for hybrid cloud environments Rapid: Machine learning for human analysis Emerging: Mixed Reality Analytics

CONCLUSION

This strategic plan demonstrates the directorate's commitment to deliver effective and innovative insight, methods, and solutions for the critical needs of the HSE. Taking into consideration the ever-changing nature of threats, R&D advances, and stakeholder needs, S&T leadership considers this plan to be a living document. As a result, S&T will continuously monitor progress on efforts described within the plan and update it as needed. In conclusion, S&T believes that with sufficient resourcing, this strategic plan will enable us to continue building upon a distinguished track record of excellence in delivering results to our HSE end users.

This page is intentionally left blank.

Homeland Security

Science and Technology