DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2017

WEDNESDAY, APRIL 6, 2016

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 2:36 p.m., in room SD–138, Dirksen Senate Office Building, Hon. John Hoeven (chairman) presiding.

Present: Senators Hoeven, Shaheen, and Tester.

DEPARTMENT OF HOMELAND SECURITY

SCIENCE AND TECHNOLOGY DIRECTORATE

STATEMENT OF HON. DR. REGINALD BROTHERS, UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY

OPENING STATEMENT OF SENATOR JOHN HOEVEN

Senator HOEVEN. The subcommittee will come to order. Good afternoon to all of you.

I would like to welcome our ranking member, Senator Shaheen. Thank you for being here and joining us.

Also, Senator Tester, thank you for joining us as well.

Senator Cochran will be joining us in a bit, and there may be some other members of the subcommittee that will be joining us as well.

I want to thank and welcome all of our witnesses today. Thank you very much for your work, and thank you for being here today, Dr. Reggie Brothers, Under Secretary for Science and Technology; Dr. Kathryn Brinsfield, Director of the Office of Health Affairs; and also Dr. Huban Gowadia—I hope I said that right; if not, correct me—Director of the Domestic Nuclear Detection Office (DNDO). So thanks to all of you for being here and for your work.

We have called this hearing to examine research and development (R&D) efforts performed at the Department of Homeland Security (DHS). By the Department's own definition, the fiscal year 2017 request for DHS includes $636 million in R&D funding. However, a number of congressional priorities have not been identified as R&D, such as $133 million in Science and Technology (S&T) laboratory facilities, so that is one thing we will want to talk about.

As we seek to examine the effectiveness of R&D efforts, it is important to understand the level of resources being applied, what is considered operating, what is considered R&D. So we hope DHS will continue to work with the subcommittee to better define its funding categories.

My focus for this hearing will be on three key areas.

First, I want to examine the metrics that you are collecting and how those measures are affecting resource decisions. How does the Department measure success in its R&D efforts? How and when do agencies decide to stop a project with interim solutions or abandon efforts that are not bearing results?

Second, this hearing is an opportunity to highlight results from R&D efforts. For example, Science and Technology's work in big data analytics transitioned from the laboratory and is generating investigative leads for Immigration and Customs Enforcement (ICE) agents, who are satisfied with this new capability.

In another example, S&T is prototyping technology that saves lives. Through a joint effort with NASA, a device called FINDER located four men trapped under 10 feet of mud and debris after an earthquake in Nepal.

Yet, for the investments that have been made in R&D at DHS since 2003, do we have the right number of success stories? What are our metrics? How do we measure success?

Third, I want to hear about projects to address emerging threats and priorities. An area of particular interest is in unmanned aerial vehicles, both in terms of countering malicious purposes by the adversaries, and as an effective force multiplier for ourselves.

Cybersecurity concerns are foremost in many of our minds, particularly as we read about possible threats of GPS spoofing and cyberattacks on airplanes, self-driving cars, and other items in the Internet of things.

One effort within the Office of Health Affairs fits within all three of the focus areas that I just outlined for this hearing—biosurveillance and detection. Today, our only civilian capability comes through BioWatch, a system to detect select biological agents in the air. Units placed in 30 cities around the country capture air samples, and then people collect and test those samples.

Unfortunately, the current BioWatch system raises issues. According to the Government Accountability Office (GAO), the units may not be deployed or sufficiently effective in the most needed locations. It takes days, in most locations, to get results. And the number of false positives leads to a lack of trust by local officials that data may not be actionable.

Several years ago, an effort to enhance BioWatch technology was abandoned. That may have been the right decision, but now we see a program continuing along a flat line in terms of capability, which does not match the threat or necessarily the need at this point.

Dr. Brinsfield's testimony points out the importance of planning, exercises, and training as part of BioWatch. DHS should work with State and local officials on those activities.

The question today is about what the technology provides and what R&D could bring to improve our biodetection and surveillance efforts.

In closing, let me just note that effective R&D programs require a skilled work force, or as my colleague, Senator Shaheen, has reminded me, people power. I think that is a direct quote.

Senator SHAHEEN. I like it.

Senator HOEVEN. It is a good one. Consisting of sharp employees who are managed and led well, and who recognize their mission.

DHS has a number of work force challenges, but we should recognize the bright spots, too. DNDO has consistently ranked as one of the best places to work in the annual Partnership for Public Service Work Force surveys.

Good work. I want to ask about how DNDO operates and the lessons other organizations in DHS can learn from its survey results.

With that, I will turn to Senator Shaheen.

STATEMENT OF SENATOR JEANNE SHAHEEN

Senator SHAHEEN. Thank you, Mr. Chairman. I would like to echo your appreciation to our three witnesses who are testifying today.

As our adversaries evolve and our environment continues to change, so too should the Department of Homeland Security. Research and development investment is one way to provide the technologies and solutions to detect, deter, and respond to the risks facing the homeland.

DHS must be strategic in how it prioritizes R&D investments to counter a myriad of threats such as cyber intrusions, plots to bring down aircraft, biological or nuclear attacks, violent extremism, and natural disasters.

Every dollar we spend in R&D has to count, and taxpayers should expect to receive a good return on investment.

Like Senator Hoeven, I was fascinated by the information about FINDER. It is the kind of innovation that I think is very exciting, as we think about what our investments might be able to do.

And I am encouraged that DHS is beginning to really explore alternative methods to solve complex problems. DHS recently set up an office in Silicon Valley to leverage the expertise of some of this country's brightest minds in technology.

Incidentally, it was interesting to see both Secretary Carter talking about using expertise from Silicon Valley to help us think about cybersecurity and other challenges facing the country, and also Secretary Kerry talking with the private sector in the media and film business to help us think about innovations there that could be helpful as we are addressing the challenges we face with countering violent extremism.

So I do think that this is a very good use of resources to think about how we better engage the private sector. The office recently awarded its first contract focused on the security of network devices.

But while there is progress, I think we also need to examine the overall spending level for DHS R&D, given the serious threats that are facing our country. Compared to other Cabinet-level agencies, DHS dedicates a very small portion of its total budget to R&D, just over 1 percent.

And we need to connect and enlist our small businesses in a robust way to help DHS address its technology demand. I know that this is something that the Secretary is very interested in doing, because small businesses are really innovators in this country. They employ nearly 40 percent of America's scientists and engineers.

They produce 14 times more patents than large businesses and universities. That is one of my favorite statistics.

Given this extraordinary track record of innovation, it makes sense to involve small businesses in developing new technologies. Plus, in New Hampshire, we have a lot of small businesses, so I like the idea that they can be part of some of this groundbreaking technology.

Finally, I think we want to learn more today about the Department's proposal to merge the Office of Health Affairs together with the Domestic Nuclear Detection Office. And I look forward to hearing more discussion about that.

So, Mr. Chairman, thank you for holding the hearing.

Thank you to our witnesses. I look forward to your testimony.

Senator HOEVEN. Thank you, Senator Shaheen.

Senator Tester, opening statement? Would you like to go ahead, so you can go to your other hearing?

Senator TESTER. I would like to hear the testimony.

Senator HOEVEN. Very good.

Under Secretary Brothers, we will begin with you.

SUMMARY STATEMENT OF HON. DR. REGINALD BROTHERS

Dr. BROTHERS. Good afternoon and thank you for this opportunity to discuss research and development in the Department of Homeland Security and the Science and Technology Directorate's budget request for fiscal year 2017.

Before I begin, I want to extend my personal thanks to the subcommittee for its partnership and assistance as I joined the Directorate almost 2 years ago. Your flexibility has allowed us to more effectively bring resources to bear on emergent needs and exigent circumstances in the Department.

The most significant result is a more robust technical advisory role to the Secretary and the components in urgent projects. Over the last 2 years, that has included work on unmanned aircraft systems (UAS), aviation security, and social media screening, among others.

The flexibility is also critical to our expansion of Apex programs and creation of Apex engines, the benefits of which we are already beginning to see in S&T in the Department.

I am grateful for your partnership and continued support moving forward.

Our research and development portfolio at the Science and Technology Directorate, or S&T, extends across diverse Homeland Security mission areas including, among others, bio, borders, cyber, transportation, first responders, and disaster resilience.

S&T is responsible for six Homeland Security labs, 10 Centers of Excellence, and 144 participating universities, and a significant support role for the Department's acquisition processes.

The portfolio must consider the full range of Homeland Security mission needs in all their considerable breadth and diversity, with a comparatively modest budget. To accomplish this, we prioritize where we spend our limited funding against hundreds of ranked capability gaps provided by end-users.

At the end of the day, we look across this set of potential projects, check what we can afford to do, where investment might make the most difference, and execute accordingly.

S&T's fiscal year 2017 funding request is vital to ensuring we can maintain our existing work on technology and knowledge products and capabilities. DHS needs to improve operational effectiveness and efficiencies.

As a research development arm and technical center of gravity for the Department, investment in innovation through S&T has significant, lasting impact on improving and maturing DHS operational capabilities and technology solutions for the Homeland Security enterprise. Likewise, a downward trend in R&D budget over time signals decreased potential for science-based and technical solutions, even as demand increases in the Department and our State and local stakeholders.

After 2 years at S&T, I am proud of how well-positioned we are. We have visionary goals that capitalize on creativity, and serve as north stars within S&T and our broader technical community. We have an updated strategy that focuses our portfolio on force-multiplying solutions. We created the first-ever S&T employee council, and we are seeing initial favorable momentum in our employee survey scores.

We see promising results from experiments with accelerators, prize competitions, and other innovative ways to reach the private sector.

One noteworthy achievement was reestablishment of the Department's integrative product teams, or IPTs. These are formal mechanisms for identifying work underway across the Department and prioritizing technological capability gaps across DHS mission areas.

Alongside existing IPTs supporting our Nation's first responders, S&T and its operational partners started five of these teams to complete these inaugural cycles in only 6 months. They validate ongoing activities and prioritize project topics in respective mission areas.

The ultimate result is better integration of S&T with DHS component activities and joint assurance through a formal report to the Secretary that technological solutions will address operational needs. The IPT process represents a major step forward for the cumulative effort across the Department.

I will close with a quick story that illustrates the evolution from capability gap to solution. Homemade explosives have emerged in last decade as materials of choice for improvised explosive devices in numerous terrorist attacks and plots. Unlike conventional threats, they are produced using household items and are difficult to detect in small but still destructive amounts.

These explosives represent one of the Department's top priorities, and are particularly relevant in wake of what we know about the recent Brussels attacks.

So what is S&T doing to move the needle? S&T begins with a need for fundamental understanding of the chemical signatures of these explosives. Since relative to other explosives, they are brand new, end-users need to know how they differ from water or shampoo in how they perform.

We work with our university and interagency partners. And once S&T has a bedrock of basic science understanding, we are to figure out safe ways to train canines, to help State and local bomb squads, to teach transportation security officers (TSOs) to find them.

Through our lab, S&T brings in the private sector to build machines and code algorithms powerful enough to see explosives wherever they are hidden.

And S&T must work with our end-users to determine the impact of all the above on operations, frontline employees, State and local enforcement, a huge list of folks who need to know this and figure out how to get technology out of labs and integrated into existing teams and complicated systems.

On top of all this, homemade explosives are a moving target. With each new threat to emerge, S&T starts again from the beginning. We activate and reactivate our subject matter experts, university researchers, lab assets, and international partners to get solutions to operate as quickly as possible.

The Transportation Security Administration (TSA), Secret Service, the Federal Protective Service, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Federal Bureau of Investigation (FBI), State and local bomb squads, canine teams, border immigration agents—these are men and women on the frontlines depending on S&T to help them stay ahead of our adversaries.

Thank you again to the subcommittee for your flexibility and support of S&T and all the work we do. I appreciate your time today, and I look forward to your questions.

[The statement follows:]

Prepared Statement of Reginald Brothers

Good afternoon Chairman Hoeven, Ranking Member Shaheen, and distinguished members of the Committee. Thank you for the opportunity to testify before you today on the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T). S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise (HSE). Technology simultaneously enables both homeland security operators and malevolent actors and, as a result, has a significant and expanding impact on current and future threat environments. I look forward to discussing S&T's fiscal year (FY) 2017 budget request and how research and development (R&D) improves the operational capabilities of DHS Components and the first responder community.

SCIENCE AND TECHNOLOGY DIRECTORATE'S FISCAL YEAR 2017 BUDGET REQUEST

S&T's budget request is $758.7 million for fiscal year 2017. This amount represents a decrease of $28.2 million, or 3.6 percent less than the $786.9 million provided to S&T in fiscal year 2016. Over the last 2 years, the flexibility afforded to S&T has allowed better responsiveness to emergent needs and exigent circumstances in the Department and contributed to a more robust technical advisory role to the Secretary and Components for urgent projects, including countering Unmanned Aircraft Systems (UAS), aviation screening, and social media screening. The flexibility was also critical to S&T's expansion of Apex programs and creation of Apex Engines, which have already begun to benefit S&T and the Department. I thank the Committee for its partnership and assistance in expanding the profile of scientific and technical advice in the Department and for its continued support moving forward in fiscal year 2017.

As part of DHS's new Common Appropriation Structure in fiscal year 2017, S&T's request aligns funding within three of the Department's lifecycle-based appropriations fund types: Research and Development; Procurement, Construction, and Improvements; and Operations and Support. S&T's fiscal year 2017 request includes no funding in the Department's fourth fund type, which is Federal Assistance.

The fiscal year 2017 budget request includes $469.9 million for R&D, a $26.1 million decrease compared to fiscal year 2016 funding. Within the requested amount, $33.0 million is for University Programs, an $8.6 million decrease, and $436.9 is for Research, Development, and Innovation, a $17.4 million decrease. By thrust area, the Research, Development, and Innovation request includes $79 million for Apex; $56 million for Border Security; $58.4 million for Chemical, Biological, and Explosives Defense; $65.7 million for Counter Terrorist; $71 million for Cyber Security and Information Analytics; $87.4 million in First Responder and Disaster Resilience; and $19.4 million for salaries and benefits. The funding in these thrust areas is S&T's principal means for providing state-of-the-art technologies and solutions and meeting broad and diverse mission requirements from throughout the Homeland Security Enterprise.

The request also includes $65.9 million for Acquisition and Operation Analysis that includes $48.4 million to fund S&T's work to strengthen the DHS acquisition process, standards development work, the SAFETY Act, international cooperative research and development, interagency work, and technology transition support and $17.5 million for salaries and benefits. To support the DHS acquisition process, S&T provides test and evaluation oversight, systems engineering, operations research, and technical risk assessments of major DHS acquisition programs.

Finally, the budget request includes $133.9 million for Laboratory Facilities, which includes $111.1 million in operations costs and $22.8 million for salaries and benefits. The request includes funding to operate the now-under-construction National Bio and Agro-Defense Facility (NBAF) located in Manhattan, KS. As construction nears completion and as research programs and veterinary research staff begin to transition from the Plum Island Animal Disease Center, NBAF will continue to require funding for operations ahead of the Full Operational Capability planned by December 2022.

SUPPORT FOR THE DEPARTMENT IN FISCAL YEAR 2017

The fiscal year 2017 funding request is vital to ensuring S&T delivers the technology knowledge products and capabilities DHS needs to improve operational effectiveness and efficiencies. In supporting end users across the broad and diverse mission areas of the Department, S&T maximizes value within a comparatively modest pool of funds. As the technical and research center for the Department, an investment in innovation through S&T has a significant, lasting impact on improving and maturing DHS operational capabilities and technology solutions for the HSE.

S&T is providing technology to strengthen border security. fiscal year 2017 funding for border security technology will provide needed capability to U.S. Customs and Border Protection (CBP) and U.S. Coast Guard (USCG). In fiscal year 2017, S&T will:

—Demonstrate a southern border capability with CBP to detect, track, and classify low flying/low observables aircraft along difficult terrain on the borders;

—Transition to CBP a covert and inexpensive capability to detect personnel, aircraft, and vehicles crossing the border with classification algorithms that significantly reduce nuisance and false alarms;

—Demonstrate a capability mounted on USCG Search and Rescue aircraft that will permit higher altitude/higher speed searches for people in the water, enabling larger coverage areas and a greater probability of detection, resulting in saved lives; and

—Pilot new or improved traveler inspection tools and processes to strengthen CBP's screening and inspection of travelers entering the United States.

S&T is testing new and existing capabilities to counter the terrorist threat. S&T is examining how to counter behavioral aspects of terrorism and how to counter emerging technology threats. S&T will evaluate mitigation technologies designed for protection at point, perimeter, and wide area venues against UAS as part of a multiagency team. The resulting testbed will deliver an urban test environment where DHS and its partners can evaluate countermeasure systems and score them against their specific operational use cases.

S&T is improving DHS acquisition programs. S&T has become an integral player in DHS improving acquisition oversight. Work in fiscal year 2017 includes:

—Technical assessments of 13 major acquisition programs in support of the Acquisition Review Board (ARB);

—Operational Test and Evaluation (OT&E) engagement with 45 major acquisition programs;

—Operations research studies in support of four DHS Components; and

—Continuous support for the Joint Requirements Council's (JRC) Portfolio Teams.

S&T is improving cybersecurity and cyber-physical systems. S&T is working to mitigate fundamental weaknesses in cyber systems. In fiscal year 2017, S&T will attack the following issues:

—Government networks retain significant cyber security weaknesses that are being exploited, and the National Cyber Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) programs need rapid and adaptive capabilities to address these weaknesses over a 12 to 24 month timeframe. fiscal year 2017 will address key elements needed to support Einstein 3A (E3A) and CDM, such as classified signatures evaluation, E3A/CDM integration, measurement infrastructure, treatment of key Internet traffic protocols and communications, and red-team capabilities.

—The government automotive fleet remains vulnerable to cyber hacking. fiscal year 2017 funding completes the establishment of the technical development consortium between DHS and major automotive companies and suppliers; it also supports Phase I development of secure purchasing guidelines for government automotive fleet management (General Services Administration, DHS including CBP, Department of Justice, state and local law enforcement, etc.).

S&T is developing better baggage scanners for aviation checkpoints. S&T is integrating new technology and more sophisticated technical approaches to create scanning machines that are faster and more dependable. In fiscal year 2017, S&T will demonstrate a carry-on baggage screener that provides better capability with higher throughput and substantially fewer false alarms. This will support the Transportation Security Administration's (TSA) efforts to secure luggage and identify threats in a less obtrusive way in the future.

S&T is supporting first responders with better communications, decisionmaking tools, and enhanced capability. S&T is working with first responders to address their most pressing capability gaps and help them do their jobs more safely and effectively. In fiscal year 2017, S&T will:

—Demonstrate a system with the Los Angeles Fire Department that uses artificial general intelligence to help responders navigate unpredictable conditions and improve situational awareness;

—Collaborate with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations to decrease the time it takes agents to identify child abuse victims and their perpetrators using imagery analytics related to facial and object recognition; and

—Operationalize a Hurricane Evacuation Planning tool with Federal Emergency Management Association (FEMA) that will streamline and automate updates for storm surge risk maps, evacuation zones, and evacuation clearance times ultimately helping local communities make faster, more efficient, and more informed evacuation decisions and save lives from hurricanes.

S&T is supporting countermeasures that protect the public from biological attacks. S&T helps our interagency partners understand the risk of potential pathogens to guide development and acquisition of countermeasures for the Strategic National Stockpile. In fiscal year 2017, S&T is delivering three material threat assessments of filoviruses, smallpox, and botulism toxin to the U.S. Department of Health and Human Services to support potential acquisition of medical countermeasures and keep the American public safe from harm.

BETTER CONNECTING S&T WITHIN THE DEPARTMENT

A significant accomplishment this year as part of the Secretary's Unity of Effort Initiative was the re-establishment of a departmental Integrated Product Team (IPT) process. In August 2015, the Secretary established mission-focused IPTs for the purpose of identifying and prioritizing technological capability gaps and coordinating R&D to close those gaps across the mission areas of the Department. The overall effort is led by S&T, but the individual IPTs are chaired by senior representatives from the operational Components, with representation from operational and HQ Components as well as the Joint Requirements Council.

The first cycle of IPTs addressed the following five topic areas: Aviation Security, Biological Threats, Counterterrorism, Border Security, and Cyber Security. S&T also continues its existing IPT supporting our Nation's first responders through the First Responder Resource Group, and additional sub-IPTs were created that address sub-topics (e.g., maritime security for border security) and key issues (e.g. resilience). This intentionally broad and inclusive approach also has helped us address some of the concerns voiced by the U.S. Government Accountability Office and Congress that R&D in the Department is insufficiently coordinated. We are on schedule to deliver results of the inaugural process to the Secretary later this year, and I am proud of how quickly S&T and our partners in the Department came together to establish and execute the process.

As they mature moving forward, IPTs will be the primary vehicle for the Department to identify, coordinate, prioritize, and validate R&D efforts supporting DHS priority missions. Most importantly, IPTs are connecting S&T more closely with the offices in Components trying to fill capability gaps and acquire technological solutions to meet operational needs. This will strengthen the applicability of S&T's deliverables and enhance the effectiveness of operational solutions for the Components.

MEETING OPERATIONAL NEEDS AND CLOSING CAPABILITY GAPS

I previously mentioned the flexibility afforded to S&T by the Committee, which has allowed better responsiveness to emergent needs and exigent circumstances in the Department. In areas such as countering Unmanned Aircraft Systems (UAS), aviation screening, and social media screening, S&T has been able to use its resources to support a more robust technical advisory role.

Last year, the Secretary requested that S&T work with the White House as interagency lead in developing a capability to counter the growing UAS threat. S&T's initial role was to lead the interagency working group including U.S. Capitol Police, U.S. Park Police, Washington DC Metropolitan Police Department, Department of Justice, Federal Aviation Administration, and DHS Components that produced the National Capital Region Gyrocopter Incident Intergovernmental After-Action Report, released June 2015, and subsequent whole-of- community response plan. Concurrently, S&T began cataloging relevant existing technology and developmental work across government including the Department of Defense. This became the basis for an R&D plan that, as it unfolds, will help drive private sector development of a capability or capabilities to meet our customers' diverse needs. Perhaps as importantly, the effort will inform our customers, to make them smarter consumers of existing and future technology, as well as the decision makers responsible for the future policy and legal framework for use of UAS.

S&T was also able to support the TSA's response to last year's results of covert testing of passenger screening operations by the DHS Office of the Inspector General. At the Secretary's request and with TSA's full cooperation, S&T was tasked to evaluate the current screening process as a risk-based "system of systems" and consider innovative or disruptive technologies, policies, and operating procedures that could improve overall screening performance and reduce risk. This effort was a horizon-focused effort that was complementary to TSA's own internal, immediate-term evaluation. With the aviation screening effort as a basis moving forward, S&T and TSA continue their close partnership in exploring and implementing innovative approaches to securing the transportation sector.

Finally, last December after the events in San Bernardino, CA, the Department stood up a Social Media Task Force led by the DHS Office of Intelligence and Analysis to assess social media policies, processes, and capabilities and to develop recommendations to leverage departmental authorities and capabilities to exploit social media during the vetting process. As one of three supporting efforts, S&T's Data Analytics Engine initiated a pilot supporting U.S. Citizenship and Immigration Services (USCIS) to address K–1 visa (i.e., fiancè/e visa) and refugee screening requirements using social media. S&T and USCIS are experimenting with leading-edge commercial tools to understand how publicly-available social media can inform the immigration vetting process. S&T has also reviewed hundreds of tools through a Request for Information and an Industry Day to determine technical capabilities available in the marketplace relative to all DHS use cases—screening and vetting, investigations, and situational awareness. S&T plans to continue to work with industry to identify and/or further develop social media analytic capabilities for DHS missions. The core technical capabilities that constitute the Apex Technology Engines help DHS rapidly develop and deploy new technologies in high-profile and high-risk events.

The technical advisory role described here is an important and sometimes underappreciated aspect of S&T's value to the Department. The immediacy of the work and difficulty to anticipate funding requirements in advance also uniquely strain our ability to marshal resources. For this once again, we are grateful to the Committee for the flexibility it affords, which augments this ability for S&T to contribute to the Department's most immediate emergent needs as they arise.

REFINEMENT AND INNOVATION IN S&T'S APPROACH TO R&D

One of my first priorities after joining S&T was establishing visionary goals that would help orient S&T's investments toward longer horizon, leap-ahead capabilities.

As demonstrated above, S&T continues to work closely with Component partners and other stakeholders on immediate needs, but the organization at the time lacked comprehensive, far-reaching visionary goals looking 20 or more years into the future and driving toward ambitious improvements. S&T shared draft goals in the Department and with the public through a crowd-sourcing website where we received more than 1,000 comments and suggestions from all of S&T's major stakeholder groups inside and outside government. The final S&T Visionary Goals, with input from the entire HSE, are the following:

—Screening at Speed: Security that Matches the Pace of Life

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

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

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

—Resilient Communities: Disaster-Proofing Society

To achieve these goals, we recognized that S&T needed to augment its approach to working with the private sector, and another of my earliest priorities at S&T was energizing a Homeland Security Industrial Base. DHS more than many Federal agencies and much more than the Department of Defense as one example, is dependent on commercially-available, off-the-shelf products to achieve its mission. Because of this, partnership with industry, specifically in product development, is essential. R&D projects can yield isolated, one-off solutions, but a truly successful portfolio must strategically shape the shelf by inserting homeland security applications, if not as primary use cases or applications, at least as considerations during companies' product development cycles.

I am proud to say that this is an area where we have enjoyed considerable success over the last 2 years. We launched innovative accelerator and prize competition platforms to reach innovators and communities that may have never heard from or worked with government before. S&T piloted an innovative program in Silicon Valley that aims to maintain constant, face-to-face contact with venture capital and start-up communities outside the Beltway including the Silicon Valley area. We developed a fresh public face by overhauling S&T's website to be more informative and transparent. Combine all of this with an updated Strategic Plan publication and willing partners within the Department including in the Management Directorate and Office of the General Counsel, and we are beginning to see real interest in the private sector in participating in a Homeland Security Industrial Base.

Accelerators

Identifying and tapping into sources of innovation is critical to our ability to support frontline operators keeping the nation safe, and accelerators (i.e., seed funding and mentorship for entrepreneur teams and start-up companies to help them attract investment) are a valuable tool to do just that. Last year, S&T piloted a business accelerator program to see if accelerators would work in the homeland security mission space. The inaugural effort, named EMERGES, focused on commercially-available wearable technology that could be adapted for first responders. More than 100 startups applied to the inaugural class, and 18 were selected and eventually featured last September at a Demo Day in San Francisco. EMERGE passed each of our initial tests, demonstrating interest in the start-up community in participation and graduation from our accelerator as well as the ability for companies to successfully develop products that attract private investment and still meet homeland security needs. More than half of EMERGE participants received interest from new private venture capital and strategic investors, three already offer commercially-available products, and one was even featured on "Shark Tank." Moving forward, we hope to build on this success in future iterations of homeland security accelerators in additional areas of work where the start-up community is ready to contribute.

Prize Competitions

Last year, S&T launched its InnoPrize program to assist DHS planning and executing prize competitions. InnoPrize utilizes America COMPETES Act authority to execute part of President's updated 2015 Strategy for American Innovation, which made it easier to use competition programs to encourage innovation, solve tough problems, and advance the core missions of the Department. This is a fresh approach to operational challenges, problem solving, and innovation aimed at problem solvers and solution makers uninterested in the burdens of traditional business with government but who otherwise are capable of helping.

S&T conducted two prize competitions in our first year of implementation, one for fresh approaches to the enduring problem of tracking first responders in GPS-degraded or denied environments and a second to seed development of a community of interest around the new National Bio and Agro-Defense Facility. Our third competition drew 58 submissions to help USCG improve navigational buoys by minimizing harmful impact to the ocean floor in environmentally-sensitive areas. Our experimentation with prize competitions in the last year has demonstrated their clear potential for widening our base of solvers and finding fresh approaches to some of the Department's enduring challenges, and I am excited to see wider use moving forward to continue infusing fresh perspective into some of our hardest problems.

Silicon Valley Presence

Building upon our existing work and partnerships in Silicon Valley, S&T is leading a departmental pilot initiative to cultivate a pipeline of non-traditional partners (e.g., start-ups) to accelerate research and innovation around homeland security priorities. Ultimately, DHS is trying to incentivize developers to widen the aperture of earlier in their development roadmaps to include homeland security solutions, again with the effect of shaping the shelf of end products available to our operators and first responders.

S&T worked closely with the DHS Office of Procurement Operations, including their Procurement Innovation Lab staff, to create an R&D-appropriate model that would keep pace with the innovation community in places like Silicon Valley. The first S&T Innovation Other Transaction Solicitation cycle focuses on securing the Internet of Things and promoting novel ideas and technologies that improve situational awareness and security for protecting domains including the 16 critical infrastructure sectors monitored by DHS. It began with an ideation workshop connecting government end users and operators with participants from the private sector (large companies, manufacturers, venture capital, researchers, and small businesses) to frame the problem and jointly shape a path forward. The first award in February, only 30 days after the solicitation, went to a team aiming to secure Internet of Things infrastructure by improving visibility and providing dynamic detection as components connect or disconnect from a system. The Internet of Things solicitation is still open, and if our Silicon Valley presence continues to benefit the Department, S&T could use it as a model to launch a similar presence in communities like Austin, Boston, and Chicago around the country.

Empowering the S&T workforce

One final aspect of S&T I ensured was not overlooked when I joined the Directorate was our organizational health and internal organization. It was clear based on conversations with S&T staff, in addition to a record of below average Federal Employee Viewpoint Survey (FEVS) scores that empowering the workforce would be critical moving forward. We performed an organizational health assessment and complementary root cause analysis to identify the most pressing areas for improvement. We stood up an S&T Employee Council to guide implementation and serve moving forward as a springboard for communication and advice for staff to leadership. Poor organizational health takes time to turn around, but improvements in S&T's most recent FEVS scores, including substantial increases in several key indices, demonstrate that S&T is moving in the right direction.

RECENT EXAMPLES OF SCIENCE AND TECHNOLOGY DIRECTORATE SUCCESSES

To conclude, here are a few examples from the Results of fiscal year 2015 Research and Development report, recently delivered to Congress, that illustrate some of the strong work in S&T's portfolio supporting DHS Components and first responders:

—In fiscal year 2015, ICE operationalized its Big Data network architecture and tools, built by S&T's Data Analytics Engine and delivered to ICE as part of the Border Enforcement Analytics Program (BEAP) Apex, for agents in three major cities. These capabilities look across multiple data sets and increase the probability of detecting illicit activity. They led to new insights and investigations and raised ICE's profile within the counter- proliferation community, creating collaboration opportunities with other agencies and partner countries.

—For first responders in fiscal year 2015, S&T licensed the Radio Internet-Protocol Communications Module (RIC–M) to two commercial partners to manufacture and sell in commercial markets. RIC–M as a low-cost interoperability solution that allows agencies to incrementally upgrade and affordably connect legacy systems with newer ones, averting a costly need to refresh entire systems at once and saving the first responder community millions of dollars. S&T was awarded a patent for the RIC–M technology and received its first royalties from RIC–M sales (seven percent of each sale made). The S&T-developed Finding Individuals for Disaster and Emergency Response (FINDER) technology also saw real-world operational use in the April 2015 Nepal earthquake response where it helped save multiple victims trapped beneath collapsed structures.

—In fiscal year 2015, S&T continued progress on the Integrated Maritime Domain Enterprise- Coastal Surveillance System (IMDE–CSS) Program for port and coastal surveillance for CBP and USCG. A Chesapeake node integrated with Maryland State and local law enforcement was linked to the original, operational Air and Marine Operations Center IMDE–CSS node in Riverside, CA. S&T continues to take major steps with its partners in USCG and CBP toward a functional, integrated system for situational awareness across all Federal, state, local, tribal, territorial, and even private sector assets.

—S&T's ten university-based Centers of Excellence continue to deliver capabilities to homeland security end users. USCG, which continues to be one of the strongest supporters and beneficiaries of the Centers, received a Social Media Analytics and Reporting Toolkit (SMART, which helps alert to emerging threats in a geographically- focused stream of social media during major events) and a new, more sophisticated version of the Boat Allocation Module (BAM II, which helps save resources and deploy more effectively across stations). FEMA received the now-operational Risk Estimator for Embankment Structures to assess and maintain levees and dams to prevent failure during future storms.

—TSA received S&T-developed systems in fiscal year 2015 that will aid implementation of classroom-based training in visual search and detection training and cross-gender empathy through appropriate hand placement and position. S&T also delivered vulnerability assessments of suicide bombers in commercial aircraft to inform in-flight emergency protocols for response and mitigation, and S&T's explosives detection canine program transitioned an S&T-developed nondetonable training aid that is considerably more affordable and effective than previous methodology at improving canine detection proficiency.

—FEMA purchased 10,000 device license subscriptions for MobileIron, effectively covering its entire inventory of working mobile devices and making MobileIron its solution of choice moving forward. MobileIron is a mobile configuration manager that improves policy enforcement and assists enterprise users in keeping their mixed-use mobile devices secure. S&T enhanced and delivered the product as part of an In-Q-Tel collaboration.

—In fiscal year 2015, S&T's Transition to Practice piloted, transitioned, or licensed five cybersecurity technologies to the marketplace. These are federally-funded tools and technologies that S&T is converting from laboratory tools to commercially-available products that will be used to strengthen our networks. S&T also continues to provide cybersecurity tools to law enforcement and delivered three tools last year that ensure computer incident evidence integrity, protect records from illicit access or modification, and verify physical location of law enforcement network-enabled mobile devices.

—In addition to technology development for Components, S&T also supports the Department's efforts to improve and integrate internal processes. In fiscal year 2015, S&T provided technical staff and support to the Joint Requirements Council (JRC) that included assistance with process development and technical subject matter expertise reach back for the JRC's Portfolio Teams. S&T also reestablished the Department's Integrated Product Team process to coordinate the Department's R&D and began a process for technical assessments of DHS major acquisitions to increase integration of acquisition and R&D activities.

—During the Ebola response in fiscal year 2015, S&T directed research at its National Biodefense Analysis and Countermeasures Center (NBACC) laboratory to determine the stability of Ebola in blood and other body fluids under relevant environmental conditions and surfaces including personal protective equipment and airline carpet. This effort, along with previous research on Ebola virus, was adopted by the White House's Ebola Task Force and influenced the approach and procedures of multiple Federal agencies during the response. USCG is also using the information to update its operational protocols for decontamination of Ebola-contaminated surfaces.

—S&T provided technical assistance to the Secret Service during the Pope Francis's September 2015 visit. S&T's Modeling and Simulation Engine generated technical oversight for crowd ingress, egress, and emergency evacuation during the Pope's visit including the outdoor mass at the Basilica of the National Shrine of the Immaculate Conception and surrounding areas. S&T's models enabled informed adjustments to congestion and bottlenecks for evacuation planning and resource positioning for the events.

I thank you again for your support and for the opportunity to testify before the Committee today on R&D in the Department and S&T's fiscal year 2017 budget. I look forward to your questions.

Senator HOEVEN. Thank you, Under Secretary.

Now, Dr. Brinsfield.

OFFICE OF HEALTH AFFAIRS

STATEMENT OF DR. KATHRYN BRINSFIELD, ASSISTANT SECRETARY AND CHIEF MEDICAL OFFICER

Dr. BRINSFIELD. Thank you, sir. Chairman Hoeven, Ranking Member Shaheen, and distinguished members of the subcommittee, I appreciate the opportunity to testify before you today regarding the Department of Homeland Security's Office of Health Affairs, or OHA.

Major threats to our Nation's security, such as terrorist attacks, natural disasters, and pandemics have profound impacts on public health. I will focus my remarks on how OHA works to mitigate the public health impacts of biological attacks, chemical threats, diseases and disasters, to help prepare the Nation to respond and rebound. I will also explain the importance of our expertise that supports DHS frontline operations, our work force, and the preparedness of public health and medical communities.

We are a crucial link between health security and homeland security. Our success is the integration of local public health with emergency management, law enforcement, and intelligence community partners.

As an example, as part of DHS and FBI's Nationwide Suspicious Activity Reporting Initiative, OHA developed a training program for health professionals to highlight the critical role they play in identifying and reporting suspicious activities.

OHA led the development of Federal guidance to help first responders manage injuries and save lives during an improvised explosive device or active shooter event. We are building on that work with Stop the Bleed, a campaign to educate Americans on actions they can take to control life-threatening bleeding before medical first responders arrive on the scene.

Like responders nationwide, DHS components also routinely confront health and medical challenges while conducting their critical missions. As part of our support to DHS operational components, OHA manages a unified emergency medical services (EMS) system for the Department's more than 3,000 emergency medical technicians (EMTs) and paramedics, and ensures the care they provide is aligned with national standards and consistent across the Department.

OHA programs also improve our Nation's ability to respond to the health impacts of chemical, biological, radiological, nuclear, and explosive incidents, or CBRNE.

These capabilities require ongoing research and development. Our role in the R&D process is to set requirements, coordinate input from State and local partners, and participate with the interagency on research priorities. This engagement is critical to addressing emerging threats.

We have all seen the news reports about ISIS's use of chemicals as weapons. We also know that they desire to attack and inspire attacks in the United States.

The most appreciable Federal impact in the immediate aftermath of a chemical attack will be made long before the incident occurs by focusing on ensuring communities are prepared to respond effectively in the first hours. OHA's chemical defense program develops guidance and tools to help U.S. communities and decisionmakers at all levels of government prepare for, respond to, and quickly recover from terrorist attacks and accidents involving toxic chemicals.

OHA also aims to improve decisionmaking about high-consequence biological threats by providing early detection and surveillance capabilities. For large-scale biological events, early knowledge will allow informed decisions that can save American lives.

The BioWatch program provides Federal, State, and local leaders with actionable information on detection of a biological event to enable a coordinated and effective response.

One important and frequently overlooked benefit of the BioWatch program is our work in each jurisdiction to ensure that local decision makers are familiar with how the response will unfold, should the detection of one of these agents happen. There is no other program that provides this layer of biological defense.

OHA and S&T are collaborating on enhancements to BioWatch that would shorten the time to detect biological agents as well as address other short- and long-term capability needs.

OHA also co-chairs S&T's biothreat IPT to identify and prioritize future needs in biodefense.

Naturally occurring biological threats can also greatly impact homeland security, as evidenced by the 2014 Ebola outbreak. As chief medical officer of the Department, I led the coordination of DHS's efforts as part of the whole-of-government response. OHA issued health advisories to help protect the DHS work force and engaged Customs and Border Protection (CBP) and the Coast Guard daily to ensure protective actions were in place so critical border security operations of the Department would continue unencumbered. Our medical professionals traveled to airports that conducted enhanced entry screening to provide advice on how to complement Ebola screening, as well as training to DHS employees on the proper use of personal protective equipment.

Further, our National Biosurveillance Integration Center, or NBIC, provided daily updates on the evolving nature of the Ebola outbreak to more than 1,500 Federal, State, and local officials, and collaborated with interagency partners on issues such as potential routes of transmission.

Today, we continue to build upon lessons learned from the responses to Ebola and other biological threats as we tackle the reemergence of viruses like Zika.

Thank you for your time. I appreciate the attention this subcommittee has given to OHA's mission, and I look forward to your questions.

[The statement follows:]

PREPARED STATEMENT OF KATHRYN H. BRINSFIELD

Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee, thank you for the opportunity to testify before you today regarding the Office of Health Affairs (OHA) and how our fiscal year 2017 budget request will allow us to further our health and homeland security missions.

Major threats to our Nation's security, such as terrorist attacks, natural disasters, or pandemics, have profound impacts on public health. The Department of Homeland Security (DHS) Office of Health Affairs leads the Department's efforts to meet those health security threats our nation faces today and prepare for the threats that will emerge tomorrow.

To us, the protection of our population is core to our mission and central to everything we do. With in-house experts including physicians, nurses, scientists, toxicologists, veterinarians, intelligence and data analysts, emergency management planners, and first responders, OHA is uniquely positioned at the intersection of public health and national security to help DHS and government leaders prepare for, respond to, and recover from the public health consequences of terrorist threats and other hazards.

OHA experts identify health and medical risks and vulnerabilities, evaluate protective actions, and understand the decisions and resources needed to effectively respond to the health impacts of terrorist attacks, large-scale disasters, and chemical and biological incidents—whether natural or intentional. We share this expertise with Federal agencies and state and local governments, to build tools, guidance, and relationships, which improve the ability of responders at all levels to coordinate and work together more effectively during a crisis.

OHA leveraged our vast expertise in support of the DHS mission to protect and secure the homeland during the 2014 Ebola outbreak. As part of the whole-of-government response, OHA led coordination of DHS's Ebola response activities, which included working closely with Departmental components, Federal interagency partners, and various state and local stakeholders. These efforts were instrumental in protecting the DHS workforce, the traveling public, and our Nation from this terrible outbreak. Today, we continue to build upon lessons learned from the responses to Ebola and other biological threats as we tackle the emergence—or reemergence—of viruses like Zika or Lassa Fever.

OHA currently addresses the health impacts of these incidents and how they impact homeland security from an integrated perspective, using both technical expertise and workforce health knowledge. OHA does not, however, conduct research and development. OHA works with the DHS Science and Technology Directorate to identify priority capability gaps in the Department's health security and chemical and biological mission spaces, and provides feedback to jointly assess challenges and prioritize solutions to fill those gaps.

The President's budget request for fiscal year 2017 will support continued and improved capabilities in these areas. In fiscal year 2017, the OHA programs and contributions discussed below are proposed to be included in a new Chemical, Biological, Radiological, Nuclear and Explosives Office. The fiscal year 2017 request will allow continued coordination and maintenance of DHS-wide chemical, biological, and emerging infectious disease-related strategy, policy, situational awareness, periodic threat and risk assessments, and contingency planning. The fiscal year 2017 request also supports our workforce health protection and Component operational resilience efforts.

OHA brings a very particular, extremely important set of skills and knowledge to our Nation's health security framework. We provide crucial links between homeland security components, public health communities, and interagency partners. We help the Nation prepare for, respond to, and recover from health impacts of homeland security threats, and we develop expert guidance and policy for the spectrum of medical and public health security issues. This unique contribution makes OHA indispensable to our Nation's security. OHA's programs and budget cost drivers are discussed below.

Chemical Defense

The Chemical Defense Program (CDP) is comprised of experts in medical toxicology, emergency medicine, industrial hygiene and public health who advise DHS and government leaders about chemical threats and the potential policy and planning consequences. CDP develops guidance and tools to help communities and decision-makers prepare for, respond to, and recover from terrorist attacks and accidents involving chemical agents. CDP provides extensive support at an extreme value, leveraging partners and resources to improve capabilities.

In 2014, CDP, in partnership with the Department of Health and Human Services and at the direction of the White House, released a guidance document to assist emergency planners and public health officials assess the medical resources needed to respond to mass casualties from a catastrophic chemical incident.

The Program has also worked directly with localities to conduct demonstration projects aimed at developing best practices for responding to chemical incidents in specific venues, such as mass transit, ports, and stadiums. In fiscal year 2014, CDP completed its first demonstration project and began development of exercises in four more venues and cities, which were all completed by the end of CY 2015. CDP is now developing a final report consolidating the identified lessons learned from the five venues and cities.

Fiscal year 2017 funding will allow CDP to continue working with communities to enhance their chemical defense capabilities by developing guidance tools and implementing the best practices and lessons learned from demonstration projects.

CDP experts will also continue to provide medical toxicology and chemical defense expertise to DHS and Component leadership and Federal government partners.

Biological Detection and Surveillance

Detection and defense against biological threats, be they acts of terrorism or naturally occurring, remain important mission areas for DHS. For large scale biological events, knowledge as early as possible allows informed decisions that can save American lives. To this end, the Department's operational biodetection and biosurveillance programs, the BioWatch Program and the National Biosurveillance Integration Center (NBIC), are critical to our Nation's biodefense. The capabilities are mutually reinforcing—one provides detection of selected threats at their onset in high risk areas while the other provides public health surveillance at a broader level at later stages. Each capability is supported by a biodefense R&D portfolio in the Science and Technology Directorate dedicated to creating technology options that address identified and validated capability gaps. R&D helps the Department maintains a longer-range view and ensures operational elements are not caught off guard by emerging or new trends and threats.

The BioWatch Program is the Nation's only civilian program that provides early warning in the event of an aerosolized biological attack. The program consists of planning, preparedness, exercising, training, and early detection capabilities. Deployed at more than 30 major metropolitan areas throughout the country, the system is a collaborative effort of health professionals at all levels of government. The program is operated by a team comprised of field operators, laboratory technicians, and public health officials from city, county, state, and Federal organizations. Each hour gained through early detection and before the onset of medical symptoms, improves the chances that response efforts will be successful.

The BioWatch Program has succeeded in bringing together state and local public health, first responders, and law enforcement personnel, along with locally-deployed Federal officials, resulting in communities that are better prepared not only for a biological attack, but also for an all-hazards response.

The current system has been, and will continue to be, extensively tested, and the program is advancing plans and building capabilities in early detection and situational awareness. BioWatch builds the collective capabilities across all levels of government to effectively and rapidly mobilize in response to an attack, mitigating the impacts of a catastrophic bioterrorism event. The BioWatch Program is a critical component of our Nation's response to minimize the impacts of a biological attack.

The relevant technical capabilities available to adversaries have only increased since the system's inception in 2003, as biotechnologies have continued their global development and dissemination. So the need for BioWatch persists. In the past 2 years, the capabilities of the system have been independently tested and validated. Four independent tests have been conducted over the last 6 years that have tested all components of the BioWatch system. This has included extensive testing of our identification assays (laboratory tests that detect selected biological agents), subsystem and system level testing in test chambers using actual threat agents, and open-air testing of simulated agents in as near an operational environment as possible. In addition, the BioWatch Quality Assurance Program has analyzed over 30,400 samples to monitor operations against performance benchmarks and requirements. The results of these tests reinforce confidence in the system's ability to achieve its mission: detecting a large-scale aerosol release of specific threat agents in our Nation's most populated areas.

The system's capability to detect biological agents was further affirmed last year when BioWatch detected the subtype of Francisella tularensis that is pathogenic to humans during confirmed occurrences of that strain of Tularemia in Denver, Colorado. Though the agent was not disseminated by an adversary, these detections took place during a documented uptick in naturally occurring disease. By analyzing available medical surveillance data and discussing the BioWatch detections through the BioWatch National Conference Call, local, state, and Federal officials were provided with additional data for decision support in responding to this occurrence of Tularemia. This shows that the BioWatch Program is able to detect an airborne biological agent in the environment.

The BioWatch Program is more than just an environmental detection system. BioWatch also helps strengthen jurisdictional preparedness in the event of a bioterrorism event through coordinating exercises and drills; providing training, guidance and assessments, and standardized methodologies for response; and by enabling a forum for all levels of government to share data and information. Over 500 state and local partners and stakeholders representing a broad cross section of government agencies have participated in BioWatch preparedness activities in the last year. BioWatch has also coordinated environmental assessment activities, including developing initial environmental sampling plans for jurisdictions to help characterize an attack. All of the program's key elements—including response—are supported by a number of Federal departments and agencies, such as the Department of Health and Human Services (HHS) including the Centers for Disease Control and Prevention (CDC), Department of Defense (DoD), Environmental Protection Agency, and Federal Bureau of Investigation. BioWatch also supports major events such as Super Bowls and National Special Security Events (e.g., 2015 papal visit to three U.S. cities).

Since 2014, BioWatch has been working with DHS S&T, DoD, and other Federal partners to identify technologies that would substantially improve BioWatch operations. These improvements are intended to advance the current "detect to treat" capability, which will enable us to deploy medical countermeasures before the affected population is symptomatic. Additionally, BioWatch and the National Biosurveillance Integration Center are working together to improve situational awareness at all levels of government in the event of a biological attack.

Given the evolving threats that our Nation faces, both manmade and natural, greater coordination among Federal, state, local, tribal, and territorial partners is required. The National Biosurveillance Integration Center, or NBIC, is uniquely situated within DHS to provide a fusion of human health, animal health, and environmental data to develop a comprehensive understanding of the biological threat landscape and emerging incidents to ensure our Nation's decision-makers have timely, accurate, and actionable information.

Established in 2004 and transitioned to OHA in 2007, NBIC's mission is to enable early warning and shared situational awareness of acute biological events and support better decisions through rapid identification, characterization, localization, and tracking for biological events of national significance. To accomplish this, NBIC monitors thousands of data sources and leverages the expertise of fourteen Federal departments and agencies, then integrates this array of information into reports on global and national biological incidents that could potentially cause economic damage, social disruption, or loss of life. Over 900 Federal and 1,500 state, local, tribal, and territorial offices across this spectrum of human, animal, and environmental health and response have access to NBIC's reports and analysis.

We are cognizant that reports by the Government Accountability Office and the Blue Ribbon Panel on Biodefense have acknowledged the progress that NBIC has made delivering daily situational awareness to our partners, but have pointed out that we still have work to do to fully realize the vision of comprehensive biosurveillance integration. Towards this end, NBIC is working with the Department of Veterans Affairs on a data initiative that will help to create an aggregated national view of disease trends, while also facilitating understanding of those trends in our veteran population. Similarly, NBIC is working with DoD's Defense Threat Reduction Agency to deploy new collaboration and analytic tools that will enable biosurveillance analysts from across the government to collaboratively examine and report on emerging biological threats. NBIC's efforts are also focused on biosurveillance tools and reporting for local officials so that they can address the biological incidents emerging in their own communities, while strengthening national surveillance as a whole. NBIC will continue to advance its capacity to conduct biosurveillance reporting and analysis by developing new collaboration tools, pursuing innovative data sources and methods, and fostering greater stakeholder engagement.

Requested fiscal year 2017 funding for the Department's biological detection and surveillance activities will enable OHA to continue biodetection operations and training in major metropolitan areas, pursue needed technological advances, and facilitate greater collaboration with Federal partners to improve the quality of national biosurveillance analysis and reporting.

Health and Emerging Infectious Diseases

The Department's workforce health protection and emerging infectious disease programs build connections between current and emerging health and medical issues. Our highly skilled health and medical experts help improve DHS planning for CBRNE threats, as well as provide expertise on medical and health issues impacting the DHS workforce and those under DHS care and custody.

OHA emergency medical services (EMS) experts are focused on improving the Nation's ability to prepare for, respond to, and recover from a terrorist attack, natural disaster, or other catastrophic emergency. We achieve this by collaborating with national organizations and government entities to help identify EMS system needs and possible solutions, engaging stakeholders nationwide, and managing an EMS system for DHS.

As an example, in 2015, OHA led the development of Federal guidance to help first responders save lives during an improvised explosive device or active shooter event. The guidance, First Responder Guidance for Improving Survivability in Improvised Explosive Device and/or Active Shooter Incidents, translates evidence-based response strategies from the U.S. military's vast experience in responding to and managing casualties from IED and/or active shooter incidents into the civilian first responder environment.

Currently, OHA is working with the White House on Stop the Bleed, a campaign to educate Americans on how to control life-threatening bleeding before emergency medical care arrives. Stop the Bleed was born out of recommendations from the National Security Council's Bystander Working Group, and was launched on October 6, 2015, at a White House stakeholder event. The Bystander Working Group was composed of both public and private sector entities. DHS is coordinating external communications for the initiative and advising on training curriculum content for bystander courses under development by Federal and nongovernmental organizations.

OHA will use fiscal year 2017 resources to continue its support for state, local, and DHS EMS systems, complete the replacement of a new electronic patient care record system for DHS EMS providers, and support a voluntary first responder anthrax vaccine pilot initiative.

OHA's health security intelligence enterprise integrates public health with law enforcement and intelligence community partners, including at state and local fusion centers and by facilitating clearances for public health stakeholders. OHA recently launched a nationwide suspicious activity reporting training program for health professionals to assist in understanding the critical role they can play in identifying and reporting suspicious activities. With requested fiscal year 2017 funding, we will continue to connect these worlds and strengthen the relationship between health and security to enhance preparedness efforts.

Finally, the DHS mission depends entirely on its greatest asset—the men and women of the Department who are responsible for keeping our Nation safe. OHA plays a key role in maintaining a healthy and resilient DHS workforce by anticipating occupational health threats and providing expert medical guidance to DHS and component leadership on medical and health issues impacting the DHS workforce. One aspect of this is the Department's Medical Countermeasures Program, which helps protect DHS workers from biological threats so that they can continue securing the homeland during a biological event. fiscal year 2017 funding will allow current occupational health activities to continue, including peer-support and stress management programs to enhance employee resilience and suicide prevention.

Conclusion

In summary, requested fiscal year 2017 funding will enable OHA to continue working to enhance the Homeland's health security capabilities by developing guidance tools and implementing best practices; strengthen the Nation's ability to anticipate, prevent, characterize, and respond to chemical or biological incidents; and continue providing the analyses, assessments, and surveillance data needed to inform and guide Federal, state, and local decisionmaking regarding the health and medical consequences of homeland security incidents.

Senator HOEVEN. Thank you.

And now, Director Gowadia.

STATEMENT OF DR. HUBAN GOWADIA, DIRECTOR

Dr. GOWADIA. Good afternoon, Chairman Hoeven, Ranking Member Shaheen, and Senator Tester. Thank you for the invitation to testify with my colleagues from the Department of Homeland Security in support of the President's 2017 budget request.

The request includes almost $152 million in the new common appropriations structure, research and development to defend the homeland against the threat of nuclear terrorism. This appropriation supports transformational applied research, detection capability and assessments, as well as nuclear forensics.

DOMESTIC NUCLEAR DETECTION OFFICE

At DNDO, our singular focus is preventing nuclear terrorism. We are charged with and committed to advancing our Nation's technological edge to deter and defeat sophisticated and agile adversaries against this threat.

In this endeavor, we are responsible by presidential directive and congressional mandate for conducting an aggressive transformational program of research and development to generate and improve technologies to detect nuclear and other radioactive materials that are out of regulatory control. We are also tasked with advancing technologies to facilitate the rapid and accurate attribution of the source of interdicted nuclear materials.

DNDO by design applies a holistic end-to-end approach to countering nuclear terrorism, beginning with a comprehensive understanding of the threat.

By integrating annual assessments of capabilities gaps and technology maturity with operational requirements, we are able to appropriately balance our resource allocations to develop material and nonmaterial solutions. We are authorized to conduct research, develop and test evaluation, and acquire radiation detectors for use by DHS operational components, such as CBP, Coast Guard, and TSA.

The President's 2017 budget request includes $104 million for acquisition of nuclear detection systems for the Department of Homeland Security.

The key to executing this end-to-end approach is DNDO's solution development process. It is our mechanism for managing programs in compliance with DHS acquisition policy and processes set forth by the Department's joint requirements council.

DNDO's process incorporates best practices for lifecycle management acquisition programs and ensures the continuous involvement of all operational partners.

When a new technology is deemed necessary to resolve a capability need, we engage with partners across the R&D community, including our Federal agencies, Department of Energy's national laboratories, academia, industry, and international partners. These collaborations allow us to leverage developments from across the science and technology community and minimize redundant efforts.

Our strategy is to fund early research to lower the technical risk and deliver mature proofs of concept to industry, enabling their investments in engineering development to deliver acquisition-ready products. Industry is thereby able to rapidly develop and improve technologies, and we are able to stimulate innovation for the nuclear detection mission.

Because DNDO is authorized and appropriated to take a comprehensive approach to this challenging mission, from threat analysis to systems acquisition, we are able to seamlessly transition technologies from bench to field for operational use, and thereby provide best value for Federal resources.

For example, DNDO led the development of the next-generation radioisotope identification device. Working closely with our partners, we identified key operational requirements that drove the new system design. Based on an enhanced detection material and improved algorithms, this new technology is easy to use, lightweight, and more reliable. Because it has built-in collaboration and diagnostics, it has much lower annual maintenance costs.

We are also seeing progress with R&D projects in nuclear forensics. For instance, DNDO recently completed the development of laboratory-scale plutonium and uranium processing capabilities that will allow us to generate nuclear forensics signatures and understand the link between material characteristics and the originating production process.

It is essential that we are able to identify the origin of these special nuclear materials to support the United States Government's commitment to hold accountable anyone that enables terrorists to obtain or use such weapons of mass destruction.

Despite significant progress, our enduring technical grand challenges remain and require sustained investment. We need cost-effective equipment with sufficient technical performance to ensure widespread deployment. We need next-generation technologies to search wide areas and capabilities for radiation scanning in challenging pathways, such as between ports of entry along our land and sea borders.

We also need technologies that can detect special nuclear material that is shielded, and enhanced technologies to rapidly and accurately determine the provenance of seized materials.

So the President's 2017 budget request includes investments in R&D to bring to bear technologies and innovation to further the Nation's nuclear detection and forensics capabilities.

Thank you for your sustained and strong support for the Department of Homeland Security efforts to counter nuclear terrorism.

[The statement follows:]

Prepared Statement of Huban A. Gowadia

Chairman Hoeven, Ranking Member Shaheen, and distinguished Members of the Subcommittee, I am honored to appear before you today to testify with my esteemed colleagues from the U.S. Department of Homeland Security (DHS) in support of the President's fiscal year (FY) 2017 Budget. The President's budget request includes $151.6 million for research and development (R&D) to defend the Homeland against the threat of radiological and nuclear terrorism. The Domestic Nuclear Detection Office (DNDO) is charged with and is committed to advancing our Nation's technological edge to defeat sophisticated and agile adversaries against this threat, principally through nuclear detection and technical nuclear forensics.

My testimony today will center on the President's fiscal year 2017 budget request for R&D under DNDO's purview, as well as the process by which we carry out these functions. It will also highlight recent accomplishments attributable to our current R&D model.

Three themes underpin my testimony. First, our R&D successes are the result of our end-to-end approach that enables a thorough understanding of the threat, operational issues, and available technologies. Second, healthy collaboration with the user community and research partners enables the exchange of information essential to make progress. Third, while we have our share of technical expertise, the critical mass of technical capability resides in our national laboratories, academia, and industry, and we have focused a great deal of our efforts to sustain the technical expertise for future advances.

MISSION AND AUTHORITIES

As stated in the President's National Security Strategy, "No threat poses as grave a danger to our security and well-being as the potential use of nuclear weapons and materials by irresponsible states or terrorists." The potentially catastrophic effects of a nuclear detonation, whether executed by a state or a non-state actor, would have far-reaching impacts on our Nation and the world.

Recognizing the grave threat of nuclear terrorism, DNDO was established in 2005 via National Security Presidential Directive (NSPD)-43/Homeland Security Presidential Directive (HSPD)-14 and subsequently authorized via the Security and Accountability For Every (SAFE) Port Act of 2006 (Public Law 109–347) to "serve as the primary entity of the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States, and improve that system over time." The National Technical Nuclear Forensics Center was established within DNDO in 2006 by NSPD–17/HSPD–4 and was authorized by the 2010 Nuclear Forensics and Attribution Act (Public Law 111–140) to "ensure an enduring national technical nuclear forensics capability to strengthen the collective response of the United States to nuclear terrorism or other nuclear attacks." DNDO is responsible for conducting an aggressive, expedited, evolutionary, and transformational program of R&D to generate and improve technologies to detect and prevent the illicit entry, transport, assembly, or potential use within the United States of a nuclear explosive device or fissile or radioactive material. DNDO is also responsible for advancing technologies to accurately and rapidly attribute the source of interdicted nuclear materials.

DNDO's R&D efforts cover four mission areas: Transformational R&D, Nuclear Forensics, Detection Capability Development, and Detection Capability Assessment.

TRANSFORMATIONAL R&D

Within Transformational R&D, DNDO manages four programs spanning basic research, applied research, and technology development:

—Advancing the fundamental knowledge in nuclear detection and forensics, the Academic Research Initiative (ARI) focuses on basic and early applied R&D to address key challenges and at the same time educate the next generation of scientists and engineers. The President's fiscal year 2017 request for the initiative is $11.8M and will include such work as transferring large solid state and no-power neutron detectors necessary for detecting nuclear material such as plutonium to industry partners for covert and extended life operations. Additionally, the budget request for the program will continue to support over 100 students at over 30 universities.

—Assessing the feasibility of promising R&D concepts, the Exploratory Research Program (ER) focuses on later applied R&D through laboratory proof-of-concept demonstrations. The budget request for the program in fiscal year 2017 is $26.1M and will include work such as the demonstration of compact and inexpensive betatron x-ray sources to enable highly mobile non-intrusive inspection systems to detect shielded threats.

—Building on R&D concepts previously demonstrated under the ER or other R&D efforts, the Advanced Technology Demonstration Program (ATD) further develops these technologies and characterizes them in a simulated or controlled operational environment to assess performance and operational utility. The President's fiscal year 2017 request is $24.1M for the Advanced Technology Demonstration program and will include work such as the operational assessment of a machine learning algorithm to further reduce nuisance alarms in radiation portal monitors.

—The purpose of the Small Business Innovation Research Program (SBIR) is to stimulate technological innovation by strengthening the role of innovative small business concerns in federally funded R&D. The program has been successful in transitioning near-term solutions into commercial products or services, such as the development of a fast neutron detector material called stilbene. In fiscal year 2017, the program will support 13 projects, which will include transitioning thallium bromide detectors for radiation pagers to a proof-of-concept.

The portfolios include materials development and supporting technology, radiation detection techniques, shielded threat detection, advanced analytics, and nuclear forensics. The President's fiscal year 2017 budget request for Transformational R&D is $64.8M.

NUCLEAR FORENSICS

DNDO's Nuclear Forensics portfolio is organized into three mission areas: operational readiness, technology advancement, and nuclear forensics expertise development. The fiscal year 2017 request for Nuclear Forensics is $20.6M and includes programs such as:

—The Technology Advancement Program benchmarks and advances forensics methodologies to provide well-understood results and develops signatures and data evaluation tools to support attribution assessments. These methods and signatures are provided to operators in the Federal Bureau of Investigation, Department of Defense, Department of Energy, and intelligence community. The President's fiscal year 2017 request is $9.6M for the Technology Advancement Program and will include such work as the operation of laboratory-scale processing capabilities that produce uranium and plutonium materials for forensics signatures.

—The National Nuclear Forensics Expertise Development Program addresses the enduring challenge of sustaining a preeminent workforce of scientists and engineers in nuclear forensics-related specialties. The program consists of Graduate Fellowships, Post-Doc Fellowships, Summer Internships, a Nuclear Forensics Research Award, and an Early-Career Award. The President's fiscal year 2017 request of $5.0M will support a total of 39 awards.

DETECTION CAPABILITY DEVELOPMENT

DNDO's Detection Capability Development portfolio addresses the development of technical solutions for detecting nuclear and other radioactive material in various operational environments and along challenging pathways. The following programs are among the activities of Detection Capability Development, for which the President has requested $21.5M:

—The International Rail Program (IRAIL) analyzes options, develops a programmatic approach for implementing solutions, and generates requirements and solutions for detecting and identifying illicit nuclear or other radioactive materials entering the United States via freight rail cargo through the 31 ports of entry identified in the Trade Act of 2002 (Public Law 107—210). The President's fiscal year 2017 request is $3.1M and will support activities for detection solutions for freight rail cargo.

—The Aerial Detection Program seeks to provide a capability via an aircraft-borne detection system during intelligence-driven operations to detect and intercept nuclear and other radioactive threats at distances far removed from major population centers and critical infrastructure, and with faster response times than interdictions made via boats and cutters. The President's fiscal year 2017 request of $3.1M will include system development activities to determine operational effectiveness and suitability of currently-available commercial products.

DETECTION CAPABILITY ASSESSMENTS

DNDO's Detection Capability Assessments portfolio supports the R&D and acquisition process for mission-related capabilities. The President's request for fiscal year 2017 for Detection Capability Assessments is $44.7M, and the following programs are a subset of those activities:

—The Test and Evaluation Program conducts rigorous assessment of radiological and nuclear detection capabilities to inform acquisition decisions and to develop and implement effective concepts of operation. The President's fiscal year 2017 request of $17.8M will include the planning, execution, and reporting of 11 test campaigns.

—The Studies and Infrastructure Program objectively assesses the effectiveness and performance of global nuclear detection architecture programs and processes. The program also supports the development and maintenance of radiological and nuclear detection standards and associated conformity testing. The President's fiscal year 2017 request is $9.4M and will include work such as the publication of advanced radiography and aerial radiation detection technical capability standards.

—The Operational Readiness Assessments Program evaluates deployed systems and operations as well as the performance of detection technologies in operationally-relevant and controlled environments. The President's fiscal year 2017 request of $8.6M will include work such as piloting a computer application that analyzes radiation portal monitor scans for reducing nuisance alarms, simplifying alarm adjudication, and increasing threat sensitivity.

STRATEGIC APPROACH

To successfully detect, interdict, and conduct nuclear forensics on nuclear and other radioactive material, it is essential that we rely on the critical triad of intelligence, law enforcement, and technology. To maximize the Nation's ability to detect and interdict a threat, it is imperative that we apply detection technologies in operations that are driven by intelligence indicators, and place them in the hands of well-trained law enforcement and public safety officials. Similarly, to enhance attribution capabilities, the U.S. Government (USG) must ensure that information from intelligence, law enforcement, and technical nuclear forensics is synthesized to identify the origin of the material or device and the perpetrators.

Addressing the threat of nuclear terrorism requires a whole-of-government approach, with partners at all levels of government. At the Federal level, U.S. Customs & Border Protection (CBP), U.S. Coast Guard (USCG), and the Transportation Security Administration play a critical role in countering nuclear threats at our borders, in aviation and maritime environments, and in our domestic transportation system. Similarly, at the state and local level, law enforcement and public safety partners are essential to the detection and interdiction of nuclear threats in their areas of operation and jurisdiction. DNDO aims to dramatically evolve nuclear detection and technical nuclear forensics capabilities and to further reduce the cost of advanced technology without causing operational burden to operators.

The initial R&D investment in nuclear and radiological detection devices is extremely more costly than most other products. It is therefore imperative that DNDO fund early research to lower the technical risk and raise the readiness of the material or technology to a point where industry is willing to absorb the remaining risk and develop a product. Thus, DNDO invests in innovative, high-risk, early-stage technologies, subsequently transitioning them to industry for commercialization. This positions DNDO to acquire fully integrated systems once they are commercially available. This approach not only enables industry to rapidly improve detection technologies and enhance existing products, but it also stimulates industry to innovate in this mission space. DNDO has successfully transferred many technologies to industry for direct commercialization.

Recognizing that some solutions may not require government development, DNDO now uses a “commercial first” acquisition strategy, engaging first with the private sector for existing solutions and only moving to a government-sponsored and managed development effort if necessary. This approach leverages industry-led innovation, takes advantage of industry’s innate flexibility and ability to rapidly improve technologies, and reduces government-funded development efforts. In some cases, shifting to commercial-based acquisitions will reduce the total time to test, acquire, and field technology.

PROCESS

DNDO applies a holistic, end-to-end approach to countering nuclear terrorism, beginning with a comprehensive understanding of the threat, including the material, the device, and the adversary. We integrate planning, research and technology development, testing and evaluation, and technology acquisition, with operational support to Federal, state, and local operators. For detection, our end-to-end approach begins with the development of an enhanced global nuclear detection architecture, which is a framework for detecting, analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control. Likewise, through the National Technical Nuclear Forensics Center, DNDO integrates planning, R&D, and operational readiness to improve the USG’s nuclear forensics capabilities.

DNDO’s approach enables seamless integration of R&D programs into the full systems engineering lifecycle from identification of a technology need to deployment of a system to the field. Our Solution Development Process provides the mechanism to manage programs in compliance with DHS acquisition life cycle stage gates, effectively integrating these programs within the appropriate governance frameworks, and successfully applying the best practices of industry and government. We are participating in the reconstituted DHS Joint Requirements Council as it works to assess joint requirements for several investment portfolios.

The Solutions Development Process is focused on the execution of an individual solution development from gap identification to post deployment activities. The first stage involves an analysis whereby gaps in the global nuclear detection architecture and technical nuclear forensics are identified and prioritized. Recognizing the continually evolving threat and the framework of defense, DNDO annually reviews multiple sources, including the global nuclear detection architecture analysis process (which includes threat modeling and risk assessment), guidance from the national technical nuclear forensics community, direct end-user interaction, recommendations from external portfolio reviews, and interactions with other USG R&D organizations.

Next, the identified gaps and needs from the first stage are translated to prioritized programmatic needs to inform DNDO’s budget formulation and decision process. The results of the gap analyses provide both concepts for specific topic areas, as well as perspective on other research areas that could broadly address a range of capability gaps. These gaps translate into the long-standing technical grand challenges, which ultimately form the research areas that make up DNDO's R&D portfolio.

In subsequent stages, a given solution progresses from planning and analysis to a selection of options. Typically, program documentation required as part of these stages include a Mission Needs Statement, Analysis of Alternatives, and Operational Requirements Documents, all of which require close end-user collaboration. As it relates to R&D, DNDO continually engages stakeholders to better understand DHS end-user operations and nuclear detection requirements to inform R&D. Following the planning and selection stages, DNDO, jointly with operators, defines solution requirements and implements design, development, and testing. This is followed by the procurement and deployment of a system based on life cycle costs. DNDO also performs a post-implementation review to examine the systems deployed to the field. At each stage of the Solutions Development Process, the Governance Review Board, comprised of DNDO leadership and operational partners, conducts corresponding reviews to assess the health of the program.

One example of a capability that matriculated through the Solutions Development Process is the development of a next-generation radioisotope identification device. We worked closely with our partners to identify key operational requirements that drove the new system design. Based on an enhanced detection material, lanthanum bromide, and improved algorithms, this new handheld technology is easy-to-use, lightweight, and more reliable. Because it has built-in calibration and diagnostics, it has a much lower annual maintenance cost.

Another example that demonstrates DNDO's end-to-end approach is the joint effort between CBP and DNDO to address the high volume of nuisance alarms generated by deployed radiation portal monitors at our ports of entry. Under DNDO's Radiation Portal Monitor Program, DNDO and CBP implemented a new approach using Revised Operational Settings (ROS) to deployed portal monitors. This collaboration and effort resulted in an average reduction of approximately 75 percent of nuisance alarms without sacrificing detector performance against threat materials, allowing officers in the field to redirect their time to other high priority law enforcement duties. The fiscal year 2017 budget request for R&D includes work to continue to improve processes to further reduce nuisance alarms.

COLLABORATIONS AND PARTNERSHIPS

Research and development of new or improved capabilities to aid in nuclear defense and countering the threat of nuclear terrorism principally rests with three organizations: DHS's DNDO, the Department of Energy (DOE) National Nuclear Security Administration's Office of Defense Nuclear Nonproliferation Research and Development, and the Department of Defense's (DoD) Defense Threat Reduction Agency. All have substantial, well-focused R&D programs that address technical gaps in threat detection and interdiction capability, focused on the unique needs of their respective mission areas and stakeholders. Further, the Office of the Director of National Intelligence plays an important intelligence and operational role in supporting the interagency research agenda.

The interagency works jointly to assure the highest caliber research is solicited and selected by the Federal Government. These activities include advance sharing of potential research topics, and supporting each other's solicitation processes through technical advice and joint proposal reviews. Specific recent examples include collaborations with the Defense Advanced Research Project Agency (DARPA) SIGMA program on distributed radiation detection networks and DNDO's collaboration with the New York City Police Department on the Radiation Awareness and Interdiction Network (RAIN) Advanced Technology Demonstration.

Within DHS, DNDO collaborates and coordinates with the USCG R&D Center and the Science and Technology Directorate (S&T), which performs R&D to support other DHS mission areas such as explosive detection. Some of the technologies developed by S&T can be utilized to detect radiological or nuclear threats. For example, if S&T develops a Non-Intrusive Inspection (NII) x-ray scanner to more effectively detect drugs, explosives, or other contraband, these devices may also be effective in detecting radiological and nuclear threats. Further, DNDO also fully and actively supports relevant Integrated Product Teams led by S&T, including one on border security.

DNDO also works closely with international partners on R&D through bilateral project arrangements. Two examples include:

—United Kingdom: DNDO and the U.K. Home Office are jointly developing and evaluating three transformational imaging and radiation detection technologies for cargo scanning at ports of entry and departure, one of which is also in collaboration with S&T.

—Singapore: DNDO and the Singapore Ministry of Home Affairs conducted an operational trial in Singapore of the DNDO developed RadMap System, which can detect and localize radioactive materials while moving, as well as overlay radiation data with visual and laser imaging data to enable a 3D reconstruction of the environment.

DNDO continues to work with international stakeholders with similar radiological and nuclear detection goals and national capabilities in the area of R&D. Leveraging agreements between DHS and foreign organizations will allow DNDO to identify areas of mutual concern and compare research portfolios to minimize overlap in parallel efforts and maximize the breadth of R&D being done across mutual portfolios.

MEASURING PROGRESS

To gauge the success of DNDO's R&D programs we internally track metrics that are indicative of progress and sponsor external reviews to assess the health and balance of our R&D portfolio. DNDO internally tracks the following metrics: program milestones, technology readiness level advancements, publications in peer-reviewed journals, presentations at recognized scientific conferences, intellectual property, licenses for software, awards in recognition of scientific achievements, and the number of students supported. Some of these metrics provide information about the progress and technological maturity of the projects and can also be used to assess the viability of technology transitions. Others indicate the ability to disseminate information to the broader scientific community and give insight into DNDO's efforts to cultivate the next generation of scientists and engineers for the nuclear-related missions. For example, DNDO's Chief Scientist patented a method and device for detecting moving radiation sources. The technique detects radioactive sources that are in motion and facilitates the rapid and accurate identification of the source of radioactive material. This invention is intended for use at seaports and border crossings that screen cargo containers, vehicles, or pedestrians for nuclear or other radioactive materials and in mobile radiation detectors deployed in search operations.

Additionally, we sponsor external reviews of our R&D portfolio and will continue to do so in the future. For example, in 2013 and 2015, DNDO sponsored reviews by an independent party to assess DNDO's existing R&D plan and portfolio, evaluating the composition, positioning, and health of the portfolio as a whole against the strategic objectives of DNDO. The review committee consisted of subject matter experts, customers, interagency R&D partners, and DNDO management.

ACCOMPLISHMENTS

Over the last several years DNDO investments in R&D have resulted in technologies that have transitioned from laboratories to commercial products used for homeland security. Some of those examples are listed below:

—Neutron Detectors for Portal Monitors: DNDO research directly facilitated the development of new materials to address the critical shortage of helium-3, the primary material used by radiation detectors to detect neutrons.[1] Several different concepts were developed and evaluated, e.g., boron-coated straw proportional counters, and are now commercially available. The alternative materials outperform helium-3 and are less expensive and more sustainable.

—Combined Gamma and Neutron Detector Material: DNDO research directly facilitated the development of cesium lithium yttrium chloride (CLYC), a single scintillator material capable of both gamma and neutron detection.[2] Previously two different detector materials had to be used, and sensors using CLYC are now commercially available in detectors that are more compact, lower power, lower cost, and more rugged than in the past. Due to its ability to detect neutrons as well as gamma rays, CLYC now stands as a viable helium-3 replacement for handheld detectors.

—Small Business-Developed Detector Material: Through the Small Business Innovation Research Program, DNDO supported the development of an improved

[1] Neutrons, in addition to gamma-rays, are key indicators of materials used in nuclear weapons.

[2] Some nuclear materials emit more gamma rays, and others emit more neutrons. Having one detector material that is sensitive to both of these primary emissions is advantageous.

process for the manufacture of stilbene, a fast neutron detector material.[3] This is now available in the United States at lower cost and with improved performance. Previously, it had only been available from sources in the Ukraine.

—Automated Threat Recognition Software: The DNDO-developed Auto-ZTM algorithm analyzes X-ray radiography images of cargo to identify the objects that may be high-Z materials[4] and provides a visual "alarm" to the operator, noting the suspicious objects in the image. To date, CBP has acquired and fielded 11 systems that are equipped with Auto-ZTM.

—Networked Detectors: Prior DNDO efforts related to an Intelligent Radiation Sensor System led to new electronics, advanced algorithms, and cell phone integration, enabling commercially available networked radiation detection systems to be used for improved wide- area search capabilities. Some of this technology is also being evaluated by DNDO in collaboration with the DARPA via their SIGMA program.

—Enabling Imaging Technology: DNDO R&D facilitated the integration of compact dual- energy x-ray generators with improved density discrimination and higher shielding penetration into commercially available mobile radiography systems.

—Plutonium and Uranium Processing Capability: DNDO supported the development of a laboratory-scale plutonium processing capability to produce plutonium materials for forensics signature development. In addition, a similar, laboratory-scale uranium processing capability completed by DNDO is now operating to produce uranium materials for signature development.

NEXT GENERATION OF SCIENTISTS AND ENGINEERS

DNDO also supports the next generation of scientists and engineers needed to execute the mission. DNDO invests in such expertise through the Academic Research Initiative by supporting areas such as advanced materials, nuclear engineering, radiochemistry, and deterrence theory. Since inception in 2007, DNDO has awarded 77 grants to 50 academic institutions, and supported over 400 students.

DNDO's National Nuclear Forensics Expertise Development Program is another effort to grow and sustain the scientific expertise required to execute the national technical nuclear forensics mission. The program has been recognized by the DOE national laboratories, universities, and the interagency as a major success in restoring the pipeline of nuclear forensics scientists. Launched in 2008, this effort is a key component in preventing nuclear terrorism, and DNDO has supported over 300 students and faculty, and 27 universities, since its inception.

Currently, twenty-one students are pursuing their PhDs, along with 16 post-doctoral fellows conducting research at the laboratories. Undergraduate scholarship and summer school initiatives are proving to be effective for recruiting future PhD candidates, with 15 new undergraduate participants each year.

The program's education awards have directly sponsored nuclear forensics related curriculum development and research partnerships at 15 universities around the country, including the hiring of eight new tenure-track junior faculty members. A total of 39 new Ph.D. nuclear forensic scientists are now in the workforce as a direct result of the program, already exceeding the threshold target of 35 set for 2018. These scientists are employed at the national laboratories, Federal agencies, and U.S. universities.

TECHNICAL GRAND CHALLENGES

Despite the progress we have made in R&D, there are five technical grand challenges that require sustained investment and are reflected within DNDO's Transformational R&D portfolio:

—Cost-effective equipment with sufficient technical performance to ensure widespread deployment;

—Detection of special nuclear material, such as plutonium and uranium, even when heavily shielded;

—Enhanced wide-area searches in a variety of scenarios, to include urban and highly cluttered environments;

[3] Fast neutrons emitted by nuclear material contain energy information that is helpful in identifying the source material. The advancement in fast neutron detection could lead to better identification equipment.

[4] "Z" refers to the atomic number of an element, equal to the number of protons. "High-Z" materials include lead (Z=82), and nuclear materials like uranium (Z=92) and plutonium (Z=94), in comparison to carbon (Z=6) or nitrogen (Z=7), and are typically more dense.

—Challenging pathways, such as between ports of entry along our land and sea borders; and

—Determination of the origins and manufacturing processes of seized material.

The fact that DNDO has supported the development of detector materials that did not exist in 2005 and which are now commercially available is a testament to the end-to-end R&D model DNDO applies to the particular set of challenges for countering nuclear terrorism.

CLOSING

DNDO's R&D is targeted to transform the basic building blocks of nuclear detection and technical nuclear forensics for dramatic capability improvements. We are committed to developing technologies for our partners to assist them in conducting their mission to protect the Nation more effectively. We engage in an end-to-end process, understanding the threat and user requirements; funding research, development, testing, and evaluation; engaging with industry, academia, and the national laboratories; and supporting the operator in the field. We seek the optimal solution for the problem at hand, whether it requires basic research, an off-the-shelf component, or a non-materiel capability. We are building not only equipment and capabilities, but also a trained workforce for the future.

While we have seen significant results and promising technologies, technical challenges remain and the threat landscape continues to evolve, which necessitates continual evaluation of current and future needs and R&D investments and innovations. To this end, DNDO will continue to work with the interagency, national laboratories, international partners, industry, and academia to maximize the return on Federal investment.

Thank you for your continued interest in and support for these efforts.

Senator HOEVEN. Thank you, Director.

We will now go to questions. We will have 5-minute rounds.

Senator Tester, would you like to proceed?

BILATERAL AGREEMENTS

Senator TESTER. I would like to. Thank you, Mr. Chairman. I appreciate the flexibility.

And thank you, Ranking Member Shaheen, for the same.

We are going to stay with you, Dr. Gowadia, as long as you just got done talking. You talk in your testimony about working closely with international partners on R&D through bilateral arrangements. You specify the United Kingdom and Singapore. Can you tell me how many other international partners you have that you are working with on bilateral agreements?

Dr. GOWADIA. I do not have the exact number off the top of my head, Senator Tester. But we have U.K., Sweden, Singapore——

Senator TESTER. So what you can do is just get that to me in writing.

Dr. GOWADIA. Certainly.

[The information follows:]

The Domestic Nuclear Detection Office (DNDO) has bilateral agreements on research and development, through the U.S. Department of Homeland Security Science & Technology Directorate, with the following countries:

—Canada

—Israel

—Singapore

—Sweden

—United Kingdom

Additionally, DNDO has bilateral agreements for cooperative activity in science and technology, operations, and policy for homeland security matters, also through the Science & Technology Directorate, with the following countries:

—Australia

—Canada

—France

—Germany

—Israel
—Mexico
—Netherlands
—Singapore
—Sweden
—United Kingdom

DETECTION OF NUCLEAR MATERIAL

Senator TESTER. And if these are agreements that are in process, or if you are trying to establish them.

The second question I have for you, very briefly, in your technical grand challenges, detection of nuclear material, plutonium and uranium, even when they are heavily shielded. How close are you to being able to do that detection?

Dr. GOWADIA. Senator, we do already have capabilities where we can detect this material using active interrogation techniques, such as x-ray systems, et cetera. The goal and the challenge is to be able to do this in environments where we do not have to use 10 MeV energy rays, for example.

Senator TESTER. How close are you to getting there?

Dr. GOWADIA. It is hard to predict invention, but we have developed smaller scale systems, and we will be fielding them very shortly.

Senator TESTER. Okay.

Dr. GOWADIA. Importantly, we have developed algorithms that already ride on systems for today that can do some of this.

RANDOMIZER PROGRAM

Senator TESTER. Okay, thank you.

Under Secretary Brothers, the TSA spent about $1.4 million on a PreCheck (Pre✔™) randomizer program, a pretty simple program. I think my 11-year-old granddaughter could have probably done the program. Nonetheless, $1.4 million was spent on it.

When I was in the State legislature, we had the same problem, IT projects that we are farming out to IT companies, and it seems like we get fleeced a lot more often than we do not. I am not saying there was a fleecing on the randomizer, but the fact is that it is a pretty simple thing to be paying $1.4 million.

Could you just talk about, is most of DHS software stuff farmed out to private contractors, at this point in time?

Dr. BROTHERS. I cannot speak to the other components. I can speak to the kind of work that we do.

Senator TESTER. Yes, your IT work.

Dr. BROTHERS. We do have some IT folks internal. We do farm some of it out, as you put it, as well. A lot of the IT software we have is commercially developed.

With respect to some of the algorithm design that we might do, that is done in laboratories, small businesses, industry, et cetera.

Senator TESTER. By DHS, where they take a program and tweak it by you guys? Or do you take a standard program and does it go to an outside source for that tweaking?

Dr. BROTHERS. Typically, the way we do our job is we identify needs. We then, through standard solicitation vehicles, identify potential solution providers. And then we fund those solution providers. Then through a rigorous method of evaluating the contracting process, we——

Senator TESTER. Yes, so the solution providers are outside DHS?

Dr. BROTHERS. Yes.

Senator TESTER. The DHS opinion, and I know there are a lot of folks that want to privatize portions of government, and in some places it is the right thing to do, in IT's case, it is your position that this is more financially efficient than keeping it in-house?

Dr. BROTHERS. What I can say is that, as you probably know, there is a tremendous amount of development in the IT space right now. If you look at where industry is going, there is tremendous explosion in that type of work as well as investment of those kinds of dollars. It is hard for DHS or other government agencies to match that level of investment that the private sector has.

Senator TESTER. Okay. I got you.

It just sometimes makes me wonder. I get the off-the-shelf stuff, a program is taking care of that has already been built. There's no need to reinvent the wheel. But, oftentimes, you spend a lot of money, and we do not end up with much, to be honest with you. It is not just DHS, by the way.

LOW-FLYING RADAR

I want to continue this on low-flying radar, particularly on the northern border, but it could be everywhere, southern border, ports, Great Lakes, wherever it may be. I have been talking about this for a while. It does not seem to be gaining any traction.

But I was told that, right now, we could not detect an airplane, for the most part, on our northern border below 5,000 feet. Is that your knowledge?

Dr. BROTHERS. So I cannot speak in specifics. What I can say is our borders and maritime division has developed what they call their small and dark aircraft program. That is specifically for that type of problem. It is showing much better performance than——

Senator TESTER. I got you. So I live 100 miles from the northern border. Would you say that that northern border has access to be able to realize if there are low-flying aircraft coming across that border?

Dr. BROTHERS. Could you repeat the question, please?

Senator TESTER. I personally live 100 miles south of the Canadian line. Do we have low-flying radar on that Canadian line right now?

Dr. BROTHERS. Let me get back to you about that specifically. I want to make sure I get you the right answer.

Senator TESTER. I can tell you, and you correct me and I will correct it for the record, I do not think we do.

Here's the problem. You can take a Cessna 182 and fly it far lower than 5,000 feet, land in an airport in a small town like I come from, Big Sandy—and I do not want to tell these guys how to do this—put your credit card in the machine, just like you do at a self-service fuel pump, fill up and take off, and we would never know what the hell is going on.

So we spend a lot of money on security, and we should spend a lot of money on security, because we need to keep our citizens secure, but this seems like a no-brainer.

So could you get back to me on what is going on?

Dr. BROTHERS. More than glad to.

[The information follows:]

The radar coverage along the northern border is less than optimal below 5000 feet. However, in areas not obscured by mountainous terrain, low level coverage improves. All sensors along the Northern Border are ground-based and therefore, the curvature of the earth limits the ability to detect aircraft at lower altitudes. The most significant limitation to the coverage along the northern border is the mountainous terrain, particularly in the western United States.

Radar systems along the Northern Border are designed and sited to address the air traffic management mission, not necessarily to optimize detection of low flying aircraft of interest to the national defense and security mission. However, in areas not obscured by terrain, CBP's Air and Marine Operations Center is able to monitor some of this lower altitude air traffic. The vast majority of the aircraft crossing the northern border complies with CBP and FAA regulations. During calendar years 2013–2015, of the thousands of aircraft that crossed our northern border, there were 79 aircraft initially reported/detected as unknown, 74 of which were later determined to be non-suspicious by CBP.

Small Dark Aircraft Detection and Timely Interdiction was identified as a high-priority capability gap in the recent DHS IPT process. Going forward, S&T will continue to work with CBP and the interagency to look at ways to improve our air surveillance capabilities, including the potential use of portable, flexible, wide area sensor system that detects and accurately tracks low flying, low observable aircraft such as helicopters, ultra-lights, small fixed wing general aviation aircraft in the rugged terrain found in many areas along the Northern Border.

Senator TESTER. I am over time. Sorry, Mr. Chairman,

Senator HOEVEN. Go ahead and finish.

Senator TESTER. Keep going?

Senator HOEVEN. Yes, unless you want to come back.

BAGGAGE SCREENERS

Senator TESTER. Okay, I will do one more. I have one more question. It has to do with baggage screeners. Since you are the guy we are dealing with, Under Secretary Brothers, we will stick with you.

Baggage screening is something that I am concerned about, but I do not know that I should be concerned about it. So what I want to know is, do you believe the technology we have deployed for baggage scanners is adequate at this point in time?

Dr. BROTHERS. I think there is always the issue whenever we do a project, for example, whenever we develop a technology, there is always a tradeoff. There is always tradeoff between security, privacy, security, speed of commerce, these kinds of things. Whenever we develop technologies and standard operating procedures, we are always in that tradeoff space.

So one of the things we are working on right now is working with TSA to develop better algorithms for existing equipment. We are working with TSA to start thinking about better actual technologies in the next midterm. And then going forward, how do we think of better architecture for the entire airport?

Senator TESTER. That is good. So that was not my question, though. My question was, are the baggage scanners we have now adequate?

Dr. BROTHERS. The reason I answered that way is because it depends on what you call sufficient. There is a whole risk-based architecture we have.

Senator TESTER. I fly four legs a week. Should I be worried?

Dr. BROTHERS. I think right now, from my perspective, from a technology perspective, we have some of the best technology we have out there.

Senator TESTER. Okay. Thank you very much.

Thank you again, Mr. Chairman.

I appreciate all of your testimony. Dr. Brinsfield, I feel guilty, but we will get you next time.

MEASURING THE EFFECTS OF R&D

Senator HOEVEN. Under Secretary Brothers, I would like to start with you.

How do you measure effectiveness in your R&D efforts? That is kind of a broad question, but we can pick up with the UAS, unmanned aerial vehicle (UAV) example.

Dr. BROTHERS. Sure.

Senator HOEVEN. Take countering the threat of unmanned aerial systems by adversaries. I mean, Senator Tester brought up that example. So what are you doing? How do you deal with that threat? And how do you determine your effectiveness?

Dr. BROTHERS. Sure. Let me tell you what we have done so far. We are leading interagency in the science and technology part of understanding and mitigating the threat due to unattended air systems. So we have developed a whole-of-community response.

The whole-of-community response includes an after-action report from the gyrocopter incident when it landed at the White House. It includes operating procedures for law enforcement when they are faced with these types of incidents. And then it includes a whole technology piece as well.

So in the technology piece, we have looked at a threat chain. The threat chain is essentially identify, characterize, track, mitigate, defeat. So that is the threat chain of how we think about if we are in a situation where we are threatened with some unattended vehicle.

Then what we are doing is we are looking at each one of those areas of the threat chain and evaluating existing commercial technologies in those areas to figure out what is best.

At the same time, we are working to understand how we would use those technologies in an architecture to protect an area, for example, the National Capital Region.

So then, if you start talking about the metrics, what you are getting at, with respect to these metrics, for the counter-UAS space, that is something we are working on right now.

We had a workshop, co-hosted with the National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory. This was several months ago. At that workshop, we actually came up with a framework for what the test parameters should be for testing these types of technologies. So we are in the process of doing that right now.

Senator HOEVEN. How do you determine, then, whether you are going to continue a project or when you discontinue?

Dr. BROTHERS. Sure. So what I was getting at is what we are doing with the whole-of-community response for the counter-UAS problem. With respect to what we are doing with our portfolio right now, we have a series of review processes. The first review process is at a lower level, which really has to do with schedule and budget and technical performance.

So if we identify a problem with those, that is when we start knowing that we have to take some action.

Then we look at a higher level. The higher level starts looking at metrics such as customer buy-in; the potential impact of the capability; if there is a novel approach; the technical feasibility of this; the transition likelihood, how likely is it to actually be used by an operator; foraging, technology foraging, has the program manager actually done a good job of looking at commercial technologies to see what they can leverage from that community; and then also whether or not this is a competency development for the Department, meaning are we leading in this area or not. So that becomes a more strategic evaluation of the portfolio.

Going forward from that, then we start looking at what percentages of our products or initiatives have excellent key performance parameters. That starts giving us a sense of, okay, now, do we really have a good sense of how these things are going to perform for the intended audience?

We start talking about what percentage of these projects have been independently evaluated. There is a whole list of metrics that we have that we talk about that we evaluate these projects on, not just on an individual project basis, but also on a portfolio basis.

The reason why we do this is because what we want to be able to do is start thinking about, strategically, is our portfolio properly shaped? So, for example, if you think in terms of looking at our portfolio on axes of impact versus technical feasibility—that is, what kind of impact will they have for our operators and how technically feasible they are—then we can plot all of our projects on charts like that. That then shows us how well we are doing. Are these highly risky projects? Are they not? Can they have high impact or not?

Then we start thinking about what kind of balance we have in that space.

Additionally, we can start thinking about individual performance parameters, as I mentioned earlier. For example, the capability impact, the customer buy-in, novel approaches. Then if we start thinking about portfolio in terms of a multidimensional plot in those terms, we then compare it to other organizations, because other organizations, whether they be more operationally focused, their portfolios more conservative, or their portfolios more aggressive, they will all show up with a certain multidimensional representation, so we can compare our portfolios to those.

So now what we have is we have a process that starts at the very low level on schedule, budget, and technical feasibility, and goes up to the very strategic level.

Senator HOEVEN. I am going to come back and ask that specifically, then, in regard to technology for TSA, but I am going to turn to my ranking member first.

EVALUATING PROJECTS

Senator SHAHEEN. Thank you.

I have to say, Under Secretary Brothers, I understand that there is jargon that you use in evaluating projects, but I did not understand a thing you said just then. So give me an example that I can relate to, so that I can explain to people.

Again, I understand you have metrics, and there is jargon in the metrics that tells you something. But if I am talking to an average voter out there who says, what are they doing at DHS to prioritize funding and to figure out what works and what does not, tell me what I should tell them.

Dr. BROTHERS. Okay. Let me tell you this way. Let me try a different way, because I understand the issue with jargon, and I apologize, because I tend to use jargon too often. I am trying to break myself of that habit. I understand.

Senator SHAHEEN. I do not like acronyms either.

[Laughter.]

Dr. BROTHERS. Okay.

So one of the things that we have done, and I mentioned this in my opening statement, is we set up these integrated product teams. The purpose of these teams is to figure out what gaps we have in capabilities across the Department.

So these can be gaps in our ability to do biosurveillance, for example, and biothreats. These can be gaps in our persistent surveillance on the border. They can be security concerns in cyber. They can be aviation security concerns.

So what we do then is we convene groups of the actual operational personnel, the people who are doing the work, and say, what are your problems? We then come up with a list of what these problems are.

We then put our resources against those problems.

Now, regarding the metrics that I mentioned, the reason I brought that up is because we have a limited budget and we have a huge mission space. And so we have to figure out what the best use of the dollars. This IPT process is helping us do that. We are now focusing on things that the entire Department says are real problems.

So now all the metrics and jargon and all that stuff, I apologize for using earlier, it has to do with how well do those programs fit into those kinds of gaps that we talked about. Do they really fit those gaps? Do they really fit the operational tactics, techniques, and procedures that the operators use in their missions?

So what we do not want to do is create a technology that is not relevant to the operators. So that is part of the metrics. Is this really operational? Did we create something that can actually transition to the operator?

So can I give you an example?

Senator SHAHEEN. Please.

Dr. BROTHERS. Okay, here's a story. Let's take these. These are gloves. These are firemen gloves. So if you look at these, they are different colors, but otherwise, they do not look very different.

The point is, we talked to fire chiefs, and they told us they had a problem. They said the problem is it is hard to get these gloves on and off, particularly when these things are wet, it is hard to get these things on and off. It is particularly hard to get them on and off because we have to operate equipment. So wouldn't it be great if we could have gloves that either we don't have to take off, or if we do, they are easy to get on and off?

That may not sound like a big deal, but it is a huge deal if you are trying to fight a fire. It is a huge deal.

And so in order for something to transition, it has to meet a need. So we talked to our fire chiefs who have a need.

Not only that, it has to be affordable. So that is another metric. Is this thing affordable?

So we said there is not much difference in cost between the old ones and the new ones. These things are affordable.

So when we talk about metrics, we have to talk about: Is it solving a real problem? Is it something that the operator is going to use?

DHS APPROPRIATE R&D VERSES PRIVATE SECTOR

Senator SHAHEEN. Okay, let me stop you there, because the other question that I have is, how do we determine what is appropriate for DHS to do in terms of R&D and what is appropriate for the private sector?

So we have a company in New Hampshire, Globe Manufacturing, that does fireman suits. They do that kind of innovation on a regular basis as part of what they do. So how do you decide what is appropriate for DHS to do and what is actually out there filling a need in the private sector?

Dr. BROTHERS. Sure. So the people that we address, that do our work, it is what I call an ecosystem. So it is universities, academia, laboratories, and industry. That is small and large industry, as well. And part of our job is to figure out what part of the ecosystem best addresses these problems. That depends. It just depends.

That is part of what we call technology foraging. We have been really trying to push that even harder, how to answer the question you are talking about. How do we know if we should go to a laboratory, should we go to large industry, should we go to small industry?

You mentioned in your statement about the Silicon Valley office. That is part of our effort to reach out to nontraditional performers, because I think it is essential, particularly now that you have so many creative people all over the place, right? You mentioned small businesses, right? Why it is important to be able to reach out to them.

I have a meeting I think in May up in New England to talk about the ecosystem up there, the same thing, because it is not just Silicon Valley, it is all over the country.

We have to figure out how to do a better job of addressing this ecosystem with our problems.

INTERAGENCY COORDINATION

Senator SHAHEEN. My time is up, but can I ask another follow-up on this?

The other question that I have is how do we determine what is part of DHS's portfolio and what is part of the Centers for Disease Control and Prevention (CDC), for example, on the Zika virus?

How do you coordinate, Dr. Brinsfield, with the CDC on what they are working on and what you are working on? How do we coordinate, as you are talking about innovation, how do you coordinate with the Defense Advanced Research Projects Agency

(DARPA) in the Department of Defense (DOD), with respect to the innovation that they are doing?

So, Dr. Brinsfield, maybe you could talk a little about that.

Dr. BRINSFIELD. Sure, absolutely.

So I think we coordinate with the interagency in a number of ways. One, obviously, at a sort of senior interagency level, we get together and meet to discuss some of these issues.

We also have regular calls and meetings with our CDC counterparts. And we participate on the Department of Health and Human Services' (HHS) public health and emergency countermeasures group. So for that, we sit and we help them define what their priorities are and what we see from the Homeland Security perspective.

When we do research or when we work with S&T to do research, we are looking at very specific pieces of the puzzle, pieces that, as the blue ribbon panel defined, fall to DHS. Even prior Secretary Shalala pointed out that these are things that fall to the Homeland Security and DHS space.

For that, we are looking specifically at the environmental detection piece or how we detect biological agents in the air, and we are looking at how we coordinate human health, animal health, and environmental health into a single picture, so that we can better inform our partners, not just in the human health arena, but across government and in State and local government as well.

So we are really trying to focus specifically into those areas that are what we do at DHS.

One piece of that, you asked how we work with other agencies specific to DOD, some of the demonstration projects that the National Biosurveillance Integration Center has done work closely with DOD and have, in fact, used their biosurveillance ecosystem and are trialing and beta testing some of their other systems in a public health environment, to see if there is cross use of some of those systems.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

TSA TECHNOLOGY

Senator HOEVEN. Under Secretary Brothers, TSA Director Neffenger is working to put together people, processes, and technology, so that we have effective screening that finds and stops threats, but still is as convenient as possible for the traveling public. There is a whole variety of things that we consider, but it is putting together people, processes, and technology in the right mix to get the best results.

Technology is your area. As you know, we had the inspector general report. There are some real issues with the technology that TSA is working. What are you doing on the technology part to make this work better?

Dr. BROTHERS. As I was mentioning to Senator Tester, we are working with Admiral Neffenger. In fact, we have a meeting with him tomorrow, the working group.

This working group is to really start addressing in the near, mid, and long term what these solutions should look like.

In the very near term, we are working with industry on better software, essentially, for the machines. So there were some vulnerabilities established, and we are working with industry to develop better algorithms so that the existing machines actually work better than they are.

In the near term, or maybe the midterm I should say, we are also working on better scanning equipment. One of the challenges—I mentioned this as well—is this whole speed versus security kind of paradigm. So we are working on different types of screening technology to enable passengers to actually move more quickly through the checkpoint.

The third thing we are trying to do is start thinking about, if you actually think about the airport as a single entity, can you actually disaggregate the checkpoint? Can you take the different pieces apart and put them in different places, so that it is more convenient for the traveling public, and it still provides even greater levels of security?

This is a longer term type of approach, of course.

We are also working with TSA on what they call their technology lanes. This is at Denver and at JFK airports, where they are interested in putting in essentially a sandbox of equipment.

So we are looking at existing equipment, some of this is in Europe and other places, this could be different types of baggage handling types of equipment, in the very near term improve our capabilities in the airports.

So I think we are looking at this holistically from the entire airport, but also from the very near term of making the machines that exist right now better in place, and then adding existing technology to the checkpoint, to other parts of the airport, improving, coming up with better screening equipment, and then, like I said, going to other airport architectures.

Senator HOEVEN. So this is a very important area and an area where you can have significant impact. Do you have the resources and are you partnering with others to do all you can in this regard?

Dr. BROTHERS. I believe we do. We are partnering very well. Like I said, we are about to make sure—both the Admiral and myself will be at this meeting tomorrow. We are partnering very closely with TSA. We are also partnering very closely with industry. So we are reaching out as much as we can.

I think the questions asked earlier about how we are working with other agencies, we are working across the interagency on these kinds of issues as well.

TUNNEL DETECTION

Senator HOEVEN. How about for Customs and Border Protection and ICE in the area of tunnel detection and ground-based sensors? How are you doing?

Dr. BROTHERS. So, for example, we have an installation of an underground system, underground fiber, that can be used to detect motion, essentially, in underground tunnels. So we have that installed. It is being tested.

We have done a variety of work with underground sensors. The issue with underground sensors, quite frankly, is how you improve their probability of detection and decrease their probability of false alarm. Whether it be animals or people, we want to make sure it detects the right thing and only the right thing, because the more often we have false alarms, then it becomes an operational nightmare.

Senator HOEVEN. How are you coming?

Dr. BROTHERS. Well, there are improvements. I think unattended underground sensors have been in the works for quite some time.

Senator HOEVEN. I have been out to see them, yes. I mean, I know some of what you have out there, but you are continuing to improve?

Dr. BROTHERS. We are continuing the work, yes.

Senator HOEVEN. And you are making progress, in terms of improving on it?

Dr. BROTHERS. Exactly.

Senator HOEVEN. Thank you.

TSA RANDOMIZER APP

Senator SHAHEEN. So I want to go back to the issue that Senator Tester was raising about the randomizer app, because, according to an Associated Press (AP) story, the TSA paid IBM $336,413.59 for the mobile application development, which included the creation of the randomizer app, which someone pointed out could generally be designed in about 10 minutes for about $20.

So do you know about this? And how does something like this happen? And how do we avoid this kind of expense for something that probably could've been done for much less money?

Dr. BROTHERS. You know, Senator, I have no details on that. I think there are always challenges when people write requirements in these kinds of things, but I can't speak to that at all.

R&D EFFORTS

Senator SHAHEEN. So something like this does not necessarily go through the Science and Technology Office?

Dr. BROTHERS. I am not aware that this did.

Senator SHAHEEN. The 2017 budget proposes combining all of the chemical, biological, radiological, nuclear, and explosive operations and policy development into one office, but the research and development efforts remain split.

I do not know if this is for you, Dr. Gowadia or Under Secretary Brothers, but maybe one of you could walk us through how you divided up that portfolio and put them in different offices, while all the other operations are proposed to go in one office. What is the thinking about that?

Dr. BROTHERS. I could start. We have had a number of conversations about this.

I think there are different models of R&D, and I think the model that S&T has, because S&T is fundamentally an organization that supports the entire Department, the entire Department. When you think of an organization like that, my experience shows it is important to have an interdisciplinary center mass, meaning it is important to have people of different diverse backgrounds in proximity to one another, because, for example, when you look at different types of technologies, when you look at the advances that have been made in the biological sciences recently, a lot of those advances are because of advances in mathematics, commuter science, and these areas. And if people in these different fields weren't constantly talking, you would not have those kinds of advances.

So for the kind of crosscutting work that S&T does, I think it is important that the kind of model we have is interdisciplinary.

Now what we also talked about is the fact that Dr. Gowadia's organization is very focused. It is very focused. It is focused on a specific area. This specific area has its own specific language and technologies and things. So for that, Dr. Gowadia has an entire integrated process of R&D and acquisition.

That is my belief why there are two different processes.

Dr. GOWADIA. May I expound just a little bit?

When we were going through the process of looking at what should come into the new CBRNE office and what should not, one of the driving principles for the reorganization was to preserve programs and activities that were working. In acknowledgment of the fact that the model was working for the rad/nuke portion of the mission space, the Department decided to keep DNDO intact and move us over into the new CBRNE office to minimize disruptions to the organization while achieving the strategic reasons to do the reorganization.

Speaking from the rad/nuke perspective, and I will pick up a little bit from what Mr. Brothers mentioned, the mission has a technical element from start to finish. However, not all solutions are technical. So when we begin to look at a mission need, when all of our operational partners, whether they are within the Department, Customs and Border Protection, TSA, Coast Guard, ICE, Secret Service, or out from our State and local partners, when they bring us a mission need, we couple that with a thorough understanding of the threat, understanding of the weapons, understanding of nuclear materials, and we are able then to devise a program forward that sometimes needs new technology and sometimes does not.

Now, the best way to determine whether you want to go down one path or another is to use an interdisciplinary approach. But when I say interdisciplinary at this stage, I mean systems analysts, policy analysts, intel analysts, nuclear physicists and engineers, law enforcement, military officers. I have essentially described for you the DNDO work force.

That is the level of interaction that needs to come into place to decide how you go down the path of developing a solution.

Now once a technical solution is deemed necessary, we work with national laboratories, academia, industry. This is where the interdisciplinary measures that Mr. Brothers referred to come to bear. So we have physicists, mathematicians, chemists, all of them working together on the technical solution.

So when we look at this mission, again, from front to end, there are technical aspects woven all through the whole system. If we were to disaggregate the rad/nuke mission based on function, you would have to recreate technical expertise in multiple directorates, multiple offices across operational components. And in this day and age with scarce budgets, it just does not seem efficient to have to duplicate that capability.

Senator SHAHEEN. Well, maybe I did not ask the question very well. That was what I was trying to figure out, was why, if we are combining all of the other operational aspects of CBRNE into one office, why are we not combining the R&D part of that into that office as well? And why are we instead leaving it within Science and Technology? That is what I am trying to understand.

Dr. BROTHERS. So right now, S&T does the chem and bio work for the Department. Again, we do work for more than just the BioWatch mission, for example, for bio. We have a number of different customers. So to take that and put it into this office, it would not be an efficient use of the kind of work we do right now, because we support more than just that mission.

Senator SHAHEEN. Okay, maybe I need to go see it, because it is still not clear to me why you would not want to take the R&D that you are doing as part of that mission and move it with the rest of that operation.

Dr. BROTHERS. Because the R&D that we have is integrated with other missions, so if you move that, you would be harming the other missions as well. And we have a good working relationship with the organization, as it is, so we are able to use the technology they are developing in that R&D in the organizations as they exist. If you took it out, you would be harming other missions.

Senator SHAHEEN. Okay. Thank you.

BIOMETRIC EXIT

Senator HOEVEN. Under Secretary, DHS is working on getting the biometric exit system implemented, and it is something that we need in order to enforce against visa overstays.

Where are you in terms of technology for the biometric exit system?

Dr. BROTHERS. So right now, we have something called AEER, which is a project that we are working on with CBP, and TSA is aware of this. It is Air Entry Exit Reengineering (AEER), what it stands for, so we don't use acronyms.

Senator HOEVEN. Senator Shaheen does not like acronyms, so you are going to have to say the whole name.

[Laughter.]

Dr. BROTHERS. So the purpose of this project is to look at commercially available biometric technologies. We actually have a location in Maryland where these are all set up in checkpoint type fashion, where we evaluate not just the effectiveness of the individual technologies, but we evaluate the effectiveness of the system itself, as the process of going through the checkpoint.

Where we are right now is we have completed most of the phases for CBP. We are still working on a detailed business case analysis of the system, and that is on the exit part of things. We are now starting to work more on the entry part of things with CBP.

Senator HOEVEN. Is the system ready for implementation?

Dr. BROTHERS. Right now, CBP is scheduling field trials with technology based on the types of things we have done and the information we have given them. But they have to determine logistics and all those kinds of things. It is more than just technology. It is how you employ this in the checkpoints and these kinds of things.

Senator HOEVEN. Is AEER significantly different than the technologies that are available commercially on the market?

Dr. BROTHERS. These are commercially available technologies.

Senator HOEVEN. So you just combine them?

Dr. BROTHERS. We are combining them, right. So the issue is there are a lot of different technologies. So, for example, CBP wanted to use tablets for their operations. Because we had to test them out in this simulated environment, we found that that was not the best idea.

So there is a distinction between whether a technology by itself works versus whether it works within a complicated system. So this is taking commercially available equipment and putting it in the actual operational environment.

Senator HOEVEN. Is it ready for implementation?

Dr. BROTHERS. Technically, yes. But the issue, again, is——

Senator HOEVEN. So that is a little confusing. "Technically, yes." You have to explain that, because I am not sure what you mean when you say, "Technically, yes."

Dr. BROTHERS. So there is technology that has been evaluated as ready to use. There are additional problems with how this would actually be used in the system by operators.

So you can say there is technology that does various types of retinal scans and these kinds of things. Does it work? Yes, it does work. But the question is how would this actually work in the airport environment.

Senator HOEVEN. Absolutely. If that is what you mean by technically, we do not need technically, yes. We need a system that is ready for implementation. CBP is telling us that they are going to put it in this year, so I want to know if it is ready to go.

Dr. BROTHERS. As far as I know, they are doing field trials. They are coming up. I do not have the schedule for that. That is when this type of evaluation will be completed.

Senator HOEVEN. Give me your guesstimate.

Dr. BROTHERS. For a timeframe? I can get back to you on that. I really do not have a guesstimate on that.

Senator HOEVEN. Okay, because CBP is telling us, I believe, that they are going to be starting to implement—oh, 2018. I was a little optimistic there. They are still testing.

Dr. BROTHERS. Yes.

Senator HOEVEN. Very good.

RAD/NUC PREVENTION

Dr. Gowadia, you thought I was not going to come to you or Dr. Brinsfield, didn't you? It is just the way this is organized. It is easier for me.

Tell us how DNDO works to prevent radiological or nuclear materials from entering the United States. So how do you work to make sure they do not get in here? And what does the public need to know about this? For the public out there that has a question when it comes to nuclear material, a dirty bomb or something like that, what should they know?

Dr. GOWADIA. Sir, as the President said in his weekly address this weekend from the Nuclear Security Summit, the threat of nuclear terrorism continues to be of grave concern. And if a terrorist organization, like ISIL, were to get their hands on some material, they would surely use it.

As such, we have to work with our partners, beginning overseas. We work through the International Atomic Energy Agency (IAEA), through the State Department's Global Initiative to Counter Nuclear Terrorism, multiple fora such as that, to share best practices with our international partners, partner nations, et cetera, so that they themselves are building nuclear detection capabilities, nuclear forensics capabilities, securing their materials as well, adhering to treaties, building regulatory infrastructure, so that they can prosecute nuclear smugglers.

As nation-states pick up their own nuclear security architectures, steadily the world gets more secure. So that is the first step.

We then work right here at our borders, making sure that we have detection capabilities in the hands of our CBP officers. Almost a hundred percent of our containerized cargo is scanned for radiation detection before it is released into the country. Almost hundred percent of truck-borne cargo and vehicular traffic that comes across our northern and southern borders is scanned for radiation. All Coast Guard boarding parties carry radiation sensors. All general aviation aircraft are met with radiation sensors and CBP officers. Similarly, all TSA Visible Intermodal Prevention and Response (VIPR) teams carry radiation sensors.

We are building Federal capabilities at our borders and within our transportation systems. Then we work with our State and local partners.

Senator HOEVEN. So that is important for the public to know what you just said.

Dr. GOWADIA. Absolutely. Absolutely, sir.

We are building, steadily, a multilayered, multifaceted architecture here. So once we get to our State and local partners, they are building organic capabilities of their own. We train them, we exercise with them, we help them decide what equipment to buy, how much of it to buy. Once it is deployed, if they need alarm resolution support, we are there to help, share the information they need to know, so their awareness is at the right level, et cetera.

So what you are hearing me talk about now is a systematic approach, a layered, multifaceted approach. So very often you hear that we have to be right every time; they only have to be right once.

If we get this right, from material security, detection capabilities, laws and regulations, nuclear forensics, good consequence management, we tie all that together in a good nuclear security architecture, they have to be right so many times, increasing their operational footprint, allowing our intelligence community, our law enforcement partners to get them before they can put nuclear and other radioactive material to malevolent use.

That is the work we are doing with our Federal partners, international partners, et cetera.

Senator HOEVEN. So whether it is air, whether it is seaborne, whether it is train, whether it is truck, all cargo is scanned.

Dr. GOWADIA. No, sir. Almost all containerized cargo that comes to us through our seaports is scanned using radiation portal monitors, and the high-risk cargo is also subject to——

Senator HOEVEN. What was that, the second one?

Dr. GOWADIA. All high-risk cargo is also subject to nonintrusive inspection using x-ray systems.

Now, the important thing is——

Senator HOEVEN. First you said containerized, so all containerized?

Dr. GOWADIA. Seaborne containerized.

Senator HOEVEN. All seaborne containerized.

Dr. GOWADIA. And truck cargo that comes in across our land and seaports, yes, that, too.

Senator HOEVEN. All truck cargo, or just when there is a perceived——

Dr. GOWADIA. All truck cargo.

Senator HOEVEN. All truck cargo coming in?

Dr. GOWADIA. Yes, sir.

Senator HOEVEN. And all containerized seaborne?

Dr. GOWADIA. Almost all. It is in aviation that we are beginning to make strides slowly, aviation cargo.

Senator HOEVEN. In aviation, it is based on threat assessment?

Dr. GOWADIA. Yes, largely based on risk assessment.

Senator HOEVEN. And then for any train traffic, by and large, that is containerized now, isn't it? Anything that comes across the ocean would be. So it would be just essentially something from Canada or Mexico that is train-borne that might not be?

Dr. GOWADIA. So the train-borne cargo, and I do not have the exact number, but the vast majority of our train crossings have, again, these x-ray systems. So the trains are scanned using x-ray systems.

Nuclear material is very, very dense. On an x-ray image, you would see it as a dark spot, so there is some capability at our train crossings.

Senator HOEVEN. I am just trying to understand what is 100 percent scanned and what is threat assessment and then scanned. What I am getting is all containerized, all seaborne containerized. Trucks, trains would tend to be based on threat assessment.

Dr. GOWADIA. No. Truck cargo, all of it.

Senator HOEVEN. All of it.

Dr. GOWADIA. Train, all of it at these certain ports of entry using the x-ray systems.

What we could do for you is we could break it down——

Senator HOEVEN. So then are we just talking some of the air luggage and so forth that is not?

Dr. GOWADIA. Now air shipments that that are like FedEx and the expedited couriers, that is 100 percent scanned as well.

Senator HOEVEN. So primarily we are down to, in essence, luggage of the traveling public. Again, that is threat assessed and then scanned.

Dr. GOWADIA. I would like to pull the string just a little further on the use of technology. Technology is a critical part of the global nuclear detection architecture, but it is not the only part. It is really important that we have systems that can be brought to bear if an intelligence cue goes up, if a law enforcement officer needs it.

So our strategy is to make sure that we conduct intelligence-cued searches using the right technology in the hands of well-trained law enforcement officers, so we are building agile technologies that can go to the fight.

Senator HOEVEN. Right, I understand. It is scanning. It is a variety of technologies. But you are also working with TSA on this piece, as far as the luggage and so forth, backroom operations, those types of issues.

Dr. GOWADIA. With TSA, we are working on two fronts. First is with their VIPR teams. These are the Visible Intermodal Prevention and Response teams, the guys that go into the trains, the metros, the subways, et cetera.

And we are also working with them on the air domain awareness board. With TSA, we are looking at are there regimes that we can put in place where, given an indicator that there is a risk, we can separate the population that needs attention from the population that does not, so we are building scanning regimes for aviation as well, building out the general aviation scanning ability.

Now all CBP officers do meet general aviation that arrives with radiation scanners.

Senator HOEVEN. Okay, thank you.

Senator SHAHEEN. So if I go to the border crossing in Pittsburgh, New Hampshire, that goes from Canada to the United States, every truck that comes across that border crossing is going to be scanned for nuclear material?

Dr. GOWADIA. It would go through a radiation portal monitor and it would be scanned, yes, ma'am.

Senator SHAHEEN. And any planes that are landing anywhere in the United States, even at private airfields, are going to be met by somebody who would be able to scan for nuclear material?

Dr. GOWADIA. International general aviation aircraft are required to land within so many miles of the border, and then CBP officers meet them with radiation sensors and scan the aircraft, the luggage, the people, yes, ma'am.

BIOLOGICAL AND CHEMICAL THREAT

Senator SHAHEEN. Dr. Brinsfield, as you think about the threat from biological and chemical weapons, what are your top priorities? How do you prioritize, I guess, first of all? And then if you are looking at what we need to do to respond to that, what criteria are you using in thinking about what the highest threats are?

Dr. BRINSFIELD. So I think it is something we spend a lot of time talking and thinking about, knowing that we have to prioritize and use our resources wisely in this space. One of the things that we know from speaking with our colleagues from public discussions is that the threat really has not changed in the past decade on the bio space, whereas the risk continues, and may even be greater.

So we look at the fact that we have to continue our day-to-day operations with the BioWatch program and support of the State and local environments, but we also spend some time thinking about how we would make that system detect more potential agents, how synthetic biology or the ability to make new agents will affect our ability to detect in the next decade, how we think about how those detection capabilities are used for naturally occurring emerging infectious diseases, and how that really will change over the course of the next decade or so.

We also look at that, similarly, in surveillance.

What we have come to find is that the lessons that we would use in a biological attack get great use in all of these diseases that have come across our shores in the last few years.

So those capabilities are really agnostic, if you will, to whether it is a terrorist use or whether it is a naturally occurring disease.

Senator SHAHEEN. So in thinking about that, one of the challenges that we face in New Hampshire, and I think in many other States, is the heroin and opioid epidemic, where we have lost many more people than we anticipate losing from any of the other biological and chemical threats that we face, barring some world-threatening disaster.

So how does something like that get prioritized and talked about? Right now, it appears to me that that is not considered, along with a list of things like Ebola and the Zika virus, as being threats to the public health. Yet the impact is much more devastating than we are seeing from either of those potential threats.

So how do we look at that kind of threat and determine whether we need to increase our response to what is happening there?

Dr. BRINSFIELD. So we also participate with the Surgeon General on their national prevention council. That is one of their priorities, particularly opioids and opioid abuse.

I do not know if I mentioned that I spent 10 years working in Boston with the Boston EMF.

Senator SHAHEEN. You did not, but I saw that in your resume.

Dr. BRINSFIELD. That is actually one of the things we looked at back then, was how do you use surveillance to actually detect where there are overdoses and how that happens.

In the past, it has been a bit controversial if we used National Biosurveillance Integration Center assets to do that type of work. But I do believe that when it comes down to it, a public health emergency is a public health emergency, and we often do not know if it is caused by an infectious disease or something else.

I would appreciate the subcommittee's look and support as we start to think through how we diversify our look into some of the space.

NATURAL DISASTERS

Senator SHAHEEN. Thank you very much for that response. I think it is really critical that we take a look at how we are defining these public health emergencies and the threat that is really posed to the population.

Certainly, I think we have, as I said, this public health emergency that we have not really defined as such. So we have been very slow to respond at the level that we need to in order to provide communities and States with help that they need.

If I can continue, Mr. Chairman, that then raises the issue of natural disasters. I guess this question is for you, Under Secretary Brothers, because as we think about the resources that we are dedicating to these natural disasters, about $13.7 million I think in this year's budget proposal, natural disasters probably have a much greater impact to date than we have seen from threats from terrorism.

So given the diversity of those natural disasters, given the challenges that they pose, can you help me understand how we determine how much we dedicate to that kind of research versus some of the other areas of research within the budget proposal?

Dr. BROTHERS. Yes, so this is a hard problem, and it is a hard problem because it goes to this word called resilience. It is a difficult word, because it carries all this meaning but it is hard to actually define quantitatively. So the reason I bring that up is because, for us to start thinking about disaster response, part of that is the resilience of our infrastructure.

So we have recently reformed a science and technology advisory committee. One of the things I asked that committee to do was to give me a better sense—this is a committee of world-renowned experts in different areas. I said, you know, help me understand resilience. Help me understand, quantitatively, how do we build a resilient infrastructure, and what that means?

So that is one way I am looking at this.

The other way I am looking at this, I am talking to, for example, the Federal Emergency Management Agency (FEMA), and said, what are some of your biggest problems?

If you take kind of the confluence of natural disasters, one of the biggest problems is flooding. So if you say it is flooding, why don't we figure out what we can do with flooding, because my concern is, as you look at natural disasters, there are so many different things we could look at. How do we figure out what to focus on?

So as I am trying to understand and we are trying to get a better sense of what resiliency means, and how we do the best job of tapping that in our communities, if FEMA says, you know what, we really need to deal with flooding. We need to understand simple questions like when do we tell people to evacuate. How can we tell them earlier to evacuate or shelter in place? Simple questions, right? How do we know where flooding is going to occur based on geography and based on property records, where are properties?

So that is a program we are doing right now, trying to help FEMA do a better job of understanding relatively simple concepts like that, but that are very difficult for real decision makers.

Senator SHAHEEN. I think you are absolutely right about resiliency. It was one reason why I found it hard to understand the budget proposal, which last year included a significant amount of money to help with mitigation, which I define as another word for resiliency. It is how do we prevent and build into our infrastructure ways to avoid the worst damage when a disaster hits.

Yet there was not money in the budget for that this year. So it seems to me that the more we can do in the way of prevention resiliency, as you call it, the better prepared we are going to be when a natural disaster strikes.

Dr. BROTHERS. Agreed.

Senator SHAHEEN. Thank you, Mr. Chairman.

BIOWATCH SYSTEM

Senator HOEVEN. Dr. Brinsfield, in a biological event, decision makers need information quickly, but it must also be accurate. This provides State and local public health officials the information to take appropriate action. Is the current BioWatch system capable of providing the real-time actionable information that officials need?

Dr. BRINSFIELD. Sir, I would say, yes, and I would also say that, of course, there is more to do.

So on the yes part, two things. First, the BioWatch system has spent much time in the last several years updating and changing the assays so that the issue of what had been called false positives or detection of a biological agent that did not cause human disease, those have not happened the last several years. The assays have been changed. The system is updated, so that we have better, more useful information.

The system has also been tested. It has been tested in the laboratory. It has been tested in a controlled environment. And it has been tested in an open air environment.

And then finally, the recent uptick in tularemia, a disease that can be naturally occurring in some of the States in the United States, showed us that even though there were low levels of human disease in a number of States across the United States, the system actually picked up in the air the tularemia and correctly identified areas in States where there was tularemia in the environment.

So we look at all those different pieces to say, well, yes, the system does, in fact, work.

Now does it tell State and local decision makers everything they need to know? No, it does not. So some of the things that we are looking at is how we can use the system more effectively in an indoor environment, how we can protect, say, concert halls and stadiums. How do we work to use the system in transit or other areas? How can we actually get that information so that it can be used in a time period where decision makers can decide whether or not to stay or evacuate as opposed to what we are doing now, which is helping decision makers decide whether or not give antibiotics?

So those are some of the challenges that we look to work with S&T and hope to solve in the near future.

Senator HOEVEN. How close are you to solving it? And how much is it going to cost? Do you have the level of funding you need now to do it? You got $82 million in 2016 and you are requesting $82 million. How much of that do you need to operate? How much is going into R&D? And how soon until you get to where you need to be?

Dr. BRINSFIELD. So that number is purely for the day-to-day operations, and the continual quality assurance testing, et cetera, of the systems that currently exist.

The R&D amounts, the pieces that are working through there, the pieces that are currently outgoing to Request for Information (RFI) to provide those improvements are something that we are doing in partnership with S&T. And Dr. Brothers is actually looking at those numbers right now.

Senator HOEVEN. That sounds like a handoff.

Dr. BROTHERS. Yes. Let me make sure I have actual numbers for the R&D part of this. I may have to get back to you with that, in terms of the actual R&D numbers, if we can do that.

What I can tell you, though, is, in terms of what we are doing with respect to the R&D, we are looking at enhancements, as Dr.

Brinsfield said, to the existing system. We have both current and near-term and long-term plans for this. We have sent out a number of RFIs last year. We are about to, early next year, send out a Broad Agency Announcement (BAA).

But again, this goes to the comments we were discussing earlier about how we do the best job of reaching out to industry to understand what the best answers are. So we are in the process of doing that right now.

Senator HOEVEN. We will want to get, from both of you, your estimate of the timeline to get where Dr. Brinsfield thinks the system is meeting the need and your estimate of how much we are spending and what we will need to spend.

Dr. BROTHERS. Sure.

[The information follows:]

OHA and S&T are currently pursuing near-term enhancements (1–3 years) and long term enhancements (7–10 years). Near-term enhancements include technologies that decrease time-to-detection and enable field characterization of the released biological threat. Long-term enhancements include autonomous systems that screen indoor environments for biological threats and new laboratory platforms that rapidly confirm and characterize samples suspected of containing a biological threat. The over-arching goal of all enhancements is to decrease the time it takes to detection and characterization of a biological attack to enable decision makers to respond more rapidly.

The current level of R&D funding for the BioWatch Program is as follows:

Fiscal year 15:	$0.5M
Fiscal year 16:	$4.7M
Fiscal year 17:	$3 million

The following funding amounts are for R&D, RDT&E, and transition of technology from S&T to BioWatch.

Fiscal year 16:	$4.7M
Fiscal year 17:	$3 million

DNDO WORKPLACE SATISFACTION

Senator HOEVEN. And then, Dr. Gowadia, what are you doing over there to get the good marks on DNDO being a good place to work? Maybe we can do more of that in some of the other parts of DHS.

Dr. GOWADIA. Thank you, Senator, for acknowledging the incredible work force at DNDO.

Some of the things that I think have been our keys to success is, one, the interdisciplinary makeup that I mentioned allows the team to come together with a singular focus, look at a problem from start to finish, and actually see the needle move in the field. Nothing is more rewarding, if you'll forgive me, for a nerd than to actually know that an invention came to life, changed real action in the field, and made the life of an officer better.

So we get to do that at DNDO. It is a tremendously challenging mission. It is very, very rewarding when we are able to meet with some of these successes.

One of the things we do every year is we analyze our data. When we get our survey results, we tear it apart as a team, and we decide one, two, three things we are going to work on that year. We do a root cause analysis of where things can get better. Staff are encouraged to be candid and transparent.

One of the first things we did was to increase our survey response numbers. If your soldiers aren't talking to you, you can't really help them. So that was the first thing we changed.

We involve them in all solutions. You do not get to complain at DNDO. You get to fix it. And people get together and solve problems.

Now, we cannot always do everything, and we are very honest about that.

Again, every year when you commit to doing something, you got to see it through. And we do. It has really truly been an honor and privilege to work with this work force for, now, 11 years.

So thank you very much for acknowledging that.

INTERCONNECTED BY INTERNET

Senator HOEVEN. It is good to hear, and it is good you are getting those results. Good for you.

Two other questions, just to kind of wrap up.

Under Secretary Brothers, this goes to what we call the Internet of things, everything is so interconnected now. I mean, we live in such a technological age, do S&T and DHS more broadly look at just how interconnected everything is? And then if we have a problem in one area with the Internet or the grid or something else, how you prevent that from continuing to go through the different systems, whether it is security systems, utilities, I mean all of these things? Are there some fail-safes or kind of protection, given the incredible connectivity of the Internet of things nowadays? Everything is connected to everything else.

Dr. BROTHERS. Senator, you share our concerns. In fact, this goes to our Silicon Valley activity, where we said, what if we engage the folks who are actually doing the development work on the Internet of things and talk to them about security? What are their concerns?

What we did is we convened a working group with a lot of industry out there. We said, what do you think the problems are? What are you concerned about? And they came back with three major issues. They came back with detecting components and connections, and how do you know something is connected? They came back with authenticating components. Is this the component I think it is? Is this a good component, a bad component? And then updating, how do you update these components?

So what we did then is we actually were able to, using our collaboration with Under Secretary for management's team, able to quickly turn around in a matter of 2 to 3 months, actually, go from solicitation to contract award, which is quite a record, I think, to actually contract one company to look at the first problem. That is detecting components and connections, and look at the other ones.

I think we are also working with industry consortia on this issue. Right now, I think what we are trying to understand is what is the role we should play here, standards, for example.

So if you are looking at the IT space for cyber, the National Institute of Standards and Technology (NIST) developed a set of standards, so-called cyber framework, a framework for thinking about Independent Review Team (IRT).

So right now (IRT) is taking off. We do not want to be left behind in terms of how we think about security, and we are aggressively pushing forward in that way.

Senator HOEVEN. I think you need to be. It is a holistic approach where sometimes you can miss the forest for the trees. You have to look at the whole big picture to know, if something happens to one part of it, that you can somehow contain it.

Dr. BROTHERS. Agreed.

Senator HOEVEN. And not have it affect everything, the chain reaction aspect.

Dr. BROTHERS. Exactly.

Senator HOEVEN. I think that is in your bailiwick, if you will, thinking about that and then finding, as you say, some of the brightest people from wherever to help you.

Dr. BROTHERS. It is. We have had conversations about this whole area of complexity. When you have interconnected systems and small failures in one, how does that avalanche into larger failures in others? These are areas we are trying to invest in.

Senator HOEVEN. For any one of you, how much do you use social media to kind of gauge where you should be putting your efforts or trying to evaluate or determine a risk? Do you have people looking at social media to see what is coming?

The other thing is, when you come up with something really good, are you filing patents? Are you getting significant revenue from that?

Just kind of touch on those.

Dr. BROTHERS. Thanks for asking that.

In terms of the first question, social media, one of the things we first did when I came onboard was I was interested in defining some long-term visions. Where do we want to be in 10, 20, 30 years, so that we can well-align our investment dollars. So we started this effort called Visionary Goals.

We started by just looking internally and asking our folks, what do you think are four or five different goals we could have? We then compiled the list. We then went to the rest of the components and got their input. We said, what if we actually went to social media? Just what you are asking.

We actually got 1,500 people who registered for our site. I thought that was pretty amazing, quite frankly. They came back with a lot of really fascinating comments on what they thought was important for Homeland Security to look at.

Then we went beyond that. We said, what if we actually started a national conversation? We started a national conversation about wearables for first responders, and we are expanding that to other areas. We are actually starting as well with how to develop an ecosystem around one of our laboratories, a business ecosystem around one of our laboratories.

So I think we are getting a lot of good results from that, because one of the issues is how we communicate to our stakeholders on what our problems are and how do we listen back. We are finding that a really good process.

With respect to patents, we just received a patent award this week, so it is timely you asked the question.

This actually has to do with special tape that is used to secure cargo. We created a new process to make it even more efficient at what it does.

One of my concerns coming in is, do we take patenting seriously enough? We have now revamped our patent portfolio because S&T actually handles the patent portfolio for the entire Department. So we are looking very strongly at that.

I think when you start thinking about things like patents and all that, you are making sure that your work force is being innovative and you are trying your best to stay ahead of this very rapidly moving space.

Senator HOEVEN. Very good.

Anything, Dr. Brinsfield or Dr. Gowadia, that you want to add to that, on either social media or patents?

Dr. BRINSFIELD. So we have looked briefly at social media. We certainly participate in social media connection with our public health community. And we have also looked at social media to see if it can predict diseases, outbreaks, worked with other interagency partners on that without great usability or success so far in being able to have social media, when people use terms such as "sick" or "ill," actually predict when there is going to be a biological disease.

So it is something that we have looked at in the aggregate form, not in particular people, but in the aggregate form, without it being highly predictive at this point.

Dr. GOWADIA. Senator, we do not work directly through the social media channel, per se, but we work very closely with the intelligence community. And certainly, our law enforcement partners stay on top of intelligence indicators and cues for something that does not fit in their backyard, something that has gone amiss. And we have a very strong interagency partnership to make sure that early cues trigger the entire system.

Senator HOEVEN. Thank you.

Senator.

Senator SHAHEEN. Thank you. I just have a final question.

But before that, I want to add my congratulations to Senator Hoeven's to you, Dr. Gowadia, and DNDO for all of the good work and for the recognition.

It sort of leads me to my last question, because I understand, Dr. Brinsfield, that one of the areas of your focus is work force health.

And having watched some first responders in New Hampshire, law enforcement and firefighters, EMTs who are there on the frontlines dealing with a crisis, I appreciate their physical and mental well-being is sometimes very much affected by what they are doing on their jobs.

So can you talk a little bit about what you are seeing in your work that is important to protect the work force, both physically and mentally?

Dr. BRINSFIELD. Yes, ma'am. I think that is something that we consider very important, whether you look at it from what we should do to take care of our employees, or you look at it purely from a fiscal perspective, we need our work force to be healthy and effective, and be able to focus on their mission.

To that end, we work carefully with all the different component medical support systems, so that we give them advisories on new threats, things that they might have a need to talk to their work force about. We take particular questions from the different components on these issues. We have worked with several of the operational components to help work with doctors and have them have medical liaison officers or lead doctors in each of the components that can focus on their particular mission set and how to keep their areas safe.

We have also worked, as I have mentioned before, with the EMTs and paramedics. Most of these are dual-trained agents, EMTs or paramedics. In many areas that our agents within DHS work, this is the only medical care available to them in either the short or long range, in some places up to 4-plus hours before they can get to a regular U.S. system for medical care.

So we have worked very carefully with them to not just ensure that they are credentialed and qualified and able to do their jobs, but also that they have the particular protocols and support systems they need, if they are working in some of those more unique environments and need special support.

We also are very interested in the mental health and well-being of our work force. And I know I mentioned before I spent a long time working with first responder community and have seen years and years of examples of how wearing it is to work in this community.

So to that end, we have a program that looks specifically at those issues. We are looking at ways to bring in more expertise in this area and really build and develop on that and have good relationships with our operational component partners and hope to continue that work.

Senator SHAHEEN. Are you sharing what you learn with DOD and the Department of Veterans Affairs (VA), which is the one that comes to mind first when we think of mental health and people who are doing work in that area, because they are facing a lot of those challenges?

Dr. BRINSFIELD. Yes, ma'am. In particular, when we first started looking at this issue, we went and sat at DOD, at the Chief of Staff's regular meeting that he has on how to prevent suicide in the work force, and we worked to see if we could learn whatever lessons we could learn from DOD in this space.

We also are trying to work on some of the relationships with, say, the International Association of Chiefs of Police and others to take some of the lessons that they have learned and be able to use that.

Senator SHAHEEN. And I assume you are sharing with them what you are learning as well.

Dr. BRINSFIELD. Absolutely. One of the things that we are just beginning to look at, the National Academy of Sciences Institute of Medicine is interested in putting together a work area on this, particularly on the well-being of first responders and how this plays. That is something that we are working with at the ground floor level.

Senator SHAHEEN. Thank you.

Thank you all very much. I think the public probably has very little awareness of the Science and Technology agency within DHS, and yet you are working on some of the most innovative aspects of the challenge that we have in protecting the homeland and keeping people safe, so thank you all very much.

ADDITIONAL COMMITTEE QUESTIONS

Senator HOEVEN. This will conclude our hearing today.

We appreciate the witnesses' testimony. Again, thanks to all of you for being here and for the work you do, very important work that you do.

The hearing record will remain open for 2 weeks from today. Senators may submit written questions for the record, and we ask that the Department respond to them within a reasonable length of time.

[The following questions were not asked at the hearing, but were submitted to the Department subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR SENATOR JOHN HOEVEN

Question. In response to a question regarding whether BioWatch was capable of "providing the real-time, actionable information that officials want and need," you answered in the affirmative. According to data you have provided subcommittee staff, however, it could take 24 to 36 hours in order for a hazard to be detected. Furthermore, BioWatch has repeatedly been the subject of GAO and OIG reports regarding the quality of information provided. In order to provide the Office of Health Affairs with the appropriate resources, we must understand the effectiveness and capabilities of its programs. Could you please provide additional information to explain your response?

Answer. BioWatch is the nation's only biodetection capability that provides early warning and facilitates jurisdictional preparedness in the event of an aerozolized biological attack. The Program provides accurate and actionable information to local, state, and Federal stakeholders 12–36 hours after a release—allowing for rapid decisionmaking upon notification of a biological incident.

Early warning of a biological attack saves lives and mitigates damage. Each hour gained through early detection and before the onset of medical symptoms, improves the chances that response efforts will be successful. Early detection of a biological attack allows response officials to dispense lifesaving medical countermeasures during a critical window of time before symptoms appear in the public. If these medications are dispensed early enough, lives will be saved and many of those exposed may never even become ill. Without this detection capability, biological attacks would remain undetected for several days until symptoms began to manifest in the public. The associated delay in response would result in increased casualties and fatalities.

BioWatch provides as close to "real time" information as currently technology allows. Analysis has shown that BioWatch's current notification timeline provides sufficient warning to deploy and dispense life-saving medical countermeasures to potentially exposed people before they develop symptoms.[1] Development of technologies and methodologies to decrease the time window from attack to detection has been and remains a priority for the BioWatch Program. The DHS Office of Health Affairs (OHA) and DHS Science and Technology Directorate (S&T) are jointly developing a plan to enhance the current BioWatch system, with a major focus on decreasing the time to detect timeline. The Department will review this plan as part of the ongoing budget deliberations for fiscal year 2018.

Furthermore, the BioWatch Program provides accurate, actionable information that enables State and local officials to take prompt and appropriate response actions. The accuracy of the BioWatch data, and effectiveness of the system, has been affirmed in multiple ways. The Program's detection capabilities have been independently tested and validated by 4 testing events conducted over the last 5 years, including testing in a laboratory, in an aerosol chamber environment, and in an open air environment. The results of these tests reinforce the Department's confidence in the system's ability to perform the mission for which it was intended: detecting a large-scale aerosol release of specific threat agents in our most populous cities.

[1] Sandia National Laboratories: BioWatch Early Detection for Exposure Prevention Analysis: Task 2 & 3 Final Results July 31, 2013 (SAND2013–6711P)

Last year the BioWatch Program analyzed over 237,000 samples from across all BioWatch jurisdictions, with 8 detections that qualified as a BioWatch Actionable Result (BAR). Although a BAR does not necessarily mean that an intentional or terrorist-related release has occurred, it allows for immediate response actions to gather additional information and assess the Public Health risk, with inputs from Federal, State, and Local agencies. Recent detections that occurred in the Denver jurisdiction correctly correlated with an uptick in Tularemia (human and animal cases), a disease that can be naturally occurring in some parts of the United States. The accuracy of the BioWatch data is further affirmed by the BioWatch Quality Assurance (QA) program. The QA program has analyzed over 35,800 QA samples since 2011, enhancing defensibility and confidence in the results.

Questions Submitted by Senator Thad Cochran

Question. It is my understanding that the Department is working to identify opportunities for cost savings through performance and management reforms, including the consolidation of administrative functions. Can you provide the subcommittee with an update on your efforts to improve efficiency of operations and help the agency better accomplish its mission?

Answer. Last year, I asked my leadership at S&T to look at the organization's administrative functions and check whether there were options for cost reduction or more efficient processes. In the process, we realized it does not always make sense to pay wages based on Washington DC's high cost of living for S&T functions focused primarily on processing paperwork.

Currently, S&T is piloting an effort to locate much of the administration associated with S&T's travel at an office in Jackson, Mississippi. With a lower cost of living and a smaller S&T footprint through telework, we expect to reduce costs associated with overseeing travel by 50 percent. We scouted a location for the office space, identified staff within S&T to lead the effort, and expect the pilot to be fully up and running by the end of this calendar year.

Question. The Department's Joint Tunnel Task force is seeking innovative technologies to help Customs and Border Protection and law enforcement agencies detect illegal intrusions on our border. Are you collaborating with other Federal agencies, including the Department of Defense, to advance important research and make use of existing capabilities in this area? The Engineer Research and Development Center at the Corps of Engineers has helped develop some useful tunnel detection capabilities. How can this committee assist you in strengthening collaborations with others and transitioning these technologies into the field?

Answer. Thank you for your continued support for S&T's tunnel detection program. Our program has worked and continues to work closely with the Department of Defense (DoD) and other Federal agencies on this challenging issue. In 2010 and 2011, S&T and DoD co-funded a Joint Capability Technical Demonstration (JCTD) with the Engineer Research and Development Center (ERDC) to install and evaluate the Border Tunneling Activity Detection System (B- TADS) in the Otay Mesa area of the southern border. With ERDC, we also co-funded construction of a test tunnel at the Yuma Proving Grounds to test existing and prototype tunnel detection equipment. Working with the U.S. Geological Survey (USGS) and DoD's Defense Threat Reduction Agency (DTRA), we developed a computer model to predict the performance of prospective tunnel detection sensors. We also regularly work with subject matter experts at DoD's Joint Improvised-Threat Defeat Agency (JIDA) Tunnel Program Office and take advantage of their significant experience with domestic and foreign geology, environmental noise signatures, and performance assessments of various tunnel detection technologies. The JIDA Tunnel Program Office recently funded S&T to make performance predictions of various tunnel detection systems that could be deployed in their theater of operations. More recently, we held several technical interchange meetings with Raytheon, the developer of the B–TADS system, to explore utilizing our tunnel detection performance modeling tool to improve its system performance.

S&T's tunnel detection program is grounded on close interagency collaboration drawing on diverse expertise across the Federal government. Moving forward, we will continue to leverage resources and experience at DoD, ERDC, and elsewhere to deliver cutting edge science and new capabilities to our operators on the border.

SUBCOMMITTEE RECESS

Senator Hoeven. With that, the subcommittee stands in recess. Thanks so much.

[Whereupon, at 4:15 p.m., Wednesday, April 6, the subcommittee was recessed, to reconvene at a time subject to the call of the Chair.]