

HOW EFFECTIVE IS THE SCIENCE AND TECHNOLOGY DIRECTORATE? STAKEHOLDER PERSPECTIVES

---

---

HEARING  
BEFORE THE  
SUBCOMMITTEE ON  
EMERGENCY PREPAREDNESS,  
RESPONSE, AND COMMUNICATIONS  
OF THE  
COMMITTEE ON HOMELAND SECURITY  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED FIFTEENTH CONGRESS  
FIRST SESSION  
NOVEMBER 7, 2017  
**Serial No. 115-36**

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

29-469 PDF

WASHINGTON : 2018

---

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
PETER T. KING, New York	SHEILA JACKSON LEE, Texas
MIKE ROGERS, Alabama	JAMES R. LANGEVIN, Rhode Island
LOU BARLETTA, Pennsylvania	CEDRIC L. RICHMOND, Louisiana
SCOTT PERRY, Pennsylvania	WILLIAM R. KEATING, Massachusetts
JOHN KATKO, New York	DONALD M. PAYNE, JR., New Jersey
WILL HURD, Texas	FILEMON VELA, Texas
MARTHA MCSALLY, Arizona	BONNIE WATSON COLEMAN, New Jersey
JOHN RATCLIFFE, Texas	KATHLEEN M. RICE, New York
DANIEL M. DONOVAN, JR., New York	J. LUIS CORREA, California
MIKE GALLAGHER, Wisconsin	VAL BUTLER DEMINGS, Florida
CLAY HIGGINS, Louisiana	NANETTE DIAZ BARRAGÁN, California
JOHN H. RUTHERFORD, Florida	
THOMAS A. GARRETT, JR., Virginia	
BRIAN K. FITZPATRICK, Pennsylvania	
RON ESTES, Kansas	
VACANCY	

BRENDAN P. SHIELDS, *Staff Director*  
STEVEN S. GIAIER, *Deputy Chief Counsel*  
MICHAEL S. TWINCHEK, *Chief Clerk*  
HOPE GOINS, *Minority Staff Director*

---

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND  
COMMUNICATIONS

DANIEL M. DONOVAN, JR., New York, *Chairman*

PETER T. KING, New York	DONALD M. PAYNE, JR., New Jersey
MARTHA MCSALLY, Arizona	JAMES R. LANGEVIN, Rhode Island
JOHN H. RUTHERFORD, Florida	BONNIE WATSON COLEMAN, New Jersey
THOMAS A. GARRETT, JR., Virginia	BENNIE G. THOMPSON, Mississippi ( <i>ex officio</i> )
MICHAEL T. MCCAUL, Texas ( <i>ex officio</i> )	

KERRY A. KINIRONS, *Subcommittee Staff Director*  
MOIRA BERGIN, *Minority Subcommittee Staff Director*

# CONTENTS

	Page
STATEMENTS	
The Honorable Daniel M. Donovan, Jr., a Representative in Congress From the State of New York, and Chairman, Subcommittee on Emergency Preparedness, Response, and Communications:	
Oral Statement .....	1
Prepared Statement .....	2
The Honorable Donald M. Payne, Jr., a Representative in Congress From the State of New Jersey, and Ranking Member, Subcommittee on Emergency Preparedness, Response, and Communications:	
Oral Statement .....	3
Prepared Statement .....	4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement .....	5
WITNESSES	
Mr. Timothy Rice, Battalion Chief, Weapons of Mass Destruction Branch Coordinator, City of New York Fire Department:	
Oral Statement .....	7
Prepared Statement .....	9
Dr. Gerald W. Parker, Jr., Associate Dean for Global One Health, College of Veterinary Medicine and Biomedical Sciences, Texas A&M University:	
Oral Statement .....	11
Prepared Statement .....	13
Mr. Jake Parker, Director of Government Relations, Security Industry Association:	
Oral Statement .....	18
Prepared Statement .....	20
Mr. Reginald Brothers, Principal, The Chertoff Group, LLC, Testifying as Former Under Secretary, Science and Technology Directorate, U.S. Department of Homeland Security:	
Oral Statement .....	22
Prepared Statement .....	24



## HOW EFFECTIVE IS THE SCIENCE AND TECHNOLOGY DIRECTORATE? STAKEHOLDER PERSPECTIVES

Tuesday, November 7, 2017

U.S. HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,  
RESPONSE, AND COMMUNICATIONS,  
COMMITTEE ON HOMELAND SECURITY,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:05 a.m., in room HVC-210, Capitol Visitor Center, Hon. Daniel M. Donovan [Chairman of the subcommittee] presiding.

Present: Representatives Donovan, Payne, Langevin, and Watson Coleman.

Also present: Representative Jackson Lee.

Mr. DONOVAN. The Subcommittee on Emergency Preparedness, Response, and Communications will come to order.

The subcommittee is meeting today to receive testimony on the effectiveness of the Science and Technology Directorate at the Department of Homeland Security. I now recognize myself for an opening statement.

I want to welcome our witnesses here today to discuss an issue that is important to our homeland security: The role of the Science and Technology Directorate within the Department of Homeland Security, and the Homeland Security Enterprise. Science and Technology, by law, is the primary research and development arm of the Department. However, it seems that over 15 years since its creation, Science and Technology is still struggling to fulfill its role within DHS and the Homeland Security Enterprise.

Given the evolving threat we face from terrorist attacks, from last week's attack in New York City to powerful hurricanes and expansive wildfires, we need to ensure that there is a component or office at the Department looking for both the short-term and long-term innovative solutions to address the challenges the Nation currently faces. By design, this should be Science and Technology.

However, budget constraints and the changes to R&D priorities have restricted Science and Technology's abilities to meet its mission. The committee has heard concerns about the lack of coordination between Science and Technology and other DHS components and offices on R&D.

Additionally, in the past, it was unclear how Science and Technology prioritizes its R&D. In 2015, DHS reinstated the Integrated Product Teams Process. These teams, comprised of a cross-

section of DHS components and offices, identify capability gaps which direct Science and Technology research and development priorities. This is a step in the right direction, but more still needs to be done.

I am troubled that Science and Technology has repeatedly changed its focus, both on whether to focus on short-term technology or long-term research on larger unknown threats, and whether to deal only with DHS components or external stakeholders. This back-and-forth needs to stop, and there needs to be a candid conversation on what Science and Technology's mission should be. I hope this hearing is just the start of these conversations.

Moving forward, this subcommittee is committed to working with all relevant stakeholders as we consider the appropriate mission and structure of Science and Technology. While Science and Technology has faced constant challenges and obstacles, there are some Science and Technology programs that have made a positive impact on the Homeland Security Enterprise. The National Urban Security Technology Lab, also known as NUSTL, in New York City, serves as a Federal resource for first responders by supporting the development and testing and evaluation of new technology.

I have had the opportunity to visit NUSTL, and have seen firsthand the remarkable resources NUSTL provides for our first responders. I was very concerned that the President's fiscal year 2018 budget request proposed its closure, in addition to the closure of two other DHS labs that focus on chemical and biological threats. Now is not the time to be cutting Federal resources to counter chemical and biological threats and support for our first responders. I am pleased that the gentleman from Maryland, Mr. Delaney, and I were able to successfully restore funding for these three vital labs during the appropriations process on the floor.

I am looking forward to hearing from our witnesses on the current State of Science and Technology and its programs, and what more needs to be done to ensure that Science and Technology is an effective and efficient partner with first responders, academia, and industry, as well as DHS components and offices. I look forward to our discussion.

[The statement of Chairman Donovan follows:]

STATEMENT OF CHAIRMAN DANIEL M. DONOVAN

NOVEMBER 7, 2017

I want to welcome our witnesses here today to discuss an issue that is important to our homeland security: The role of the Science and Technology Directorate (S&T) within the Department of Homeland Security and the Homeland Security Enterprise.

S&T, by law, is the primary research and development (R&D) arm of the Department. However, it seems that over 15 years since its creation, S&T is still struggling to fulfill its role within DHS and the Homeland Security Enterprise.

Given the evolving threat we face from terrorist attacks, like last week's attack in New York City, to powerful hurricanes and expansive wildfires, we need to ensure that there is a component or office at the Department looking for both the short-term and long-term innovative solutions to address the challenges the Nation currently faces. By design, this should be S&T.

However, budget constraints and the changes to R&D priorities have restricted S&T abilities to meet its mission. The committee has heard concerns about the lack of coordination between S&T and other DHS components and offices on R&D. Additionally, in the past, it was unclear how S&T prioritized its R&D. In 2015, DHS

reinstated the Integrated Product Teams (IPTs) process. These teams, comprised of a cross-section of DHS components and offices, identify capability gaps which directs S&T R&D priorities. This is a step in the right direction, but more still needs to be done.

I am troubled that S&T has repeatedly changed its focus—both on whether to focus on short-term technology transferring or longer-term research on larger unknown threats and whether to deal only with DHS components or external stakeholders. This back-and-forth needs to stop and there needs to be candid conversations on what S&T's mission should be. I hope this hearing is just the start of these conversations. Moving forward, this subcommittee is committed to working with all relevant stakeholders as we consider the appropriate mission and structure of S&T.

While S&T has faced constant challenges and obstacles, there are some S&T programs that have made a positive impact on the Homeland Security Enterprise.

The National Urban Security Technology Laboratory (NUSTL), in New York City, serves as a Federal resource for first responders by supporting the development and testing and evaluation of new technology. I've had the opportunity to visit NUSTL and see first-hand the remarkable resources NUSTL provides to our first responders. I was very concerned that the President's fiscal year 2018 budget request proposed its closure in addition to two other DHS labs that focus on the chemical and biological threats. Now is not the time to be cutting Federal resources to counter chemical and biological threats and support for our first responders. I'm pleased that the gentlemen from Maryland, Mr. Delaney, and I were able to successfully restore funding for these three vital labs during the appropriations process on the House floor.

I'm looking forward to hearing from our witnesses on the current state of S&T and its programs and what more needs to be done to ensure S&T is an effective and efficient partner with first responders, academia, and industry as well as DHS components and offices. I look forward to our discussion.

Mr. DONOVAN. The Chair now recognizes my friend, the gentleman from New Jersey, Mr. Payne, for an opening statement that he may have.

Mr. PAYNE. Good morning. I want to thank the Chairman for holding this Subcommittee on Emergency Preparedness, Response, and Communications, first hearing to review the activities of the Science and Technology Directorate. I look forward to working with S&T and its stakeholders to ensure that components of the Department, and their State and local partners have the technology they need to do the jobs better and safer.

I would like to begin, however, by addressing a few matters not directly related to today's hearing.

First, I would like to send my sympathies to those affected by the horrific terrorist attack in New York City on Halloween, and express my gratitude to the brave firefighters, EMS, and law enforcement personnel who responded.

I would also like to join the people of Sutherland Springs, Texas in mourning the 26 people murdered for being at the wrong place at the wrong time—in this case, at church on Sunday. To those grieving loved ones, we pray for your strength in the difficult days that are to come.

To those fed up with Members of Congress sending their thoughts and prayers to victims of mass shootings every time it happens, and then refusing to do anything to stop it, I stand with you as well. Instead of letting senseless actions take place, it is long overdue that we do what makes the most sense to significantly change, or to stop this from ever happening again.

Finally, I would like to express my disappointment that last week's full committee hearing with the FEMA administrator and the mayor of San Juan was postponed, and join full committee Ranking Member Thompson in asking that it be rescheduled as

soon as possible. As I said at our last hearing, our National response doctrine is not working for the people of Puerto Rico and the U.S. Virgin Islands, and we need to figure out what we can do to expedite the response and recovery efforts there. They are American citizens as well.

I have heard first-hand from citizens attempting to get goods to struggling family members back in Puerto Rico, and finding unsurmountable financial obstacles at every single turn. We must do better, and not tomorrow—right now.

Returning to the subject of today's hearing, one thing that these recent tragedies have taught us is that the threats we face, from natural disasters to man-made attacks, are continuing to evolve. From extreme weather events becoming more frequent and more severe, to terrorists weaponizing cars and trucks, to bad actors wreaking havoc on soft targets, the kind of threats facing our country demands Science and Technology Directorate that is sufficiently innovative and dynamic to be responsive to the demands of the ever-changing threat landscape.

I want to thank all the witnesses for being here today, particularly Dr. Reggie Brothers, the former under secretary of science and technology. During the 3 years he spent leading S&T, Dr. Brothers focused on cultivating relationships with the Homeland Security industrial base to better leverage off-the-shelf technologies, coordinating research development priorities across the Department, and launching programs to attract business to work with S&T by streamlining the bureaucratic processes.

Dr. Brothers navigated tight budgets and organizational challenges within DHS to create incentives for private-sector engagement, and did so while working to overcome long-held industry concerns that S&T did not have the budget or clout within the Department to guarantee a market for homeland security solutions.

Although S&T matured under Dr. Brothers' leadership, it continues to face budget challenges, struggles to gain the confidence of the private-sector partners, and is involved in large DHS reorganizations of certain chemical, biological, and radiological and nuclear counterterrorism activities.

Now that Dr. Brothers is a free agent, no longer bound by OMB, I will be interested in his candid observations on these issues, and how the committee can help bolster S&T credibility as the research and development hub that drives acquisition decisions in the Department.

With that, I look forward to the witnesses' testimony, and I yield back the balance of my time.

[The statement of Ranking Member Payne follows:]

STATEMENT OF RANKING MEMBER DONALD M. PAYNE, JR.

NOVEMBER 7, 2017

I look forward to working with S&T and its stakeholders to ensure that components of the Department and their State and local partners have the technology they need to do their jobs better and safer.

I would like to begin, however, by addressing a few matters not directly related to today's hearing.

First, I would like to send my sympathies to those affected by the horrific terrorist attack in New York City on Halloween and express my gratitude to the brave firefighters, EMS, and law enforcement personnel who responded.

I would also like to join the people of Sutherland Springs, Texas in mourning the 26 people murdered for being at the place at the wrong time—in this case, at church on Sunday.

To those grieving loved ones, we pray for your strength in the difficult days that are to come.

And to those fed up with Members of Congress sending their thoughts and prayers to the victims of the mass shootings every time it happens and then refusing to do anything to stop it, I stand with you. Instead of letting senseless actions take place, it is long overdue that we do what makes the most sense and take significant action to stop this from ever happening again.

Finally, I would like to express my disappointment that last week's full committee hearing with the FEMA administrator and the mayor of San Juan was postponed, and join full committee Ranking Member Thompson in asking that it be rescheduled as soon as possible.

As I said at our last hearing, our National response doctrine is not working for the people of Puerto Rico and the U.S. Virgin Islands, and we need to figure out what we can do to expedite the response and recovery efforts there.

I have heard, first-hand, from citizens attempting to get goods to struggling family members back in Puerto Rico and find unsurmountable financial obstacles at every single turn. We must do better and not tomorrow, right now.

Returning to the subject of today's hearing, one thing these recent tragedies have taught us is that the threats we face—from natural disasters to man-made attacks—are continuing to evolve.

From extreme weather events becoming more frequent and more severe, to terrorists weaponizing cars and trucks, to bad actors wreaking havoc on soft targets, the kind of threats facing our country demands a Science and Technology Directorate that is sufficiently innovative and dynamic to be responsive to the demands of an ever-changing threat landscape.

I want to thank all of the witnesses for being here today, particularly Dr. Reggie Brothers, the former under secretary for science and technology.

During the 3 years he spent leading S&T, Dr. Brothers focused on cultivating relationships with the Homeland Security Industrial Base to better leverage off-the-shelf technologies, coordinating research and development priorities across the Department, and launching programs to attract businesses to work with S&T by streamlining bureaucratic processes.

Dr. Brothers navigated tight budgets and organizational challenges within DHS to create incentives for private-sector engagement and did so while working to overcome long-held industry concerns that S&T did not have the budget or clout within the Department to guarantee a market for homeland security solutions.

Although S&T matured under Dr. Brothers' leadership, it continues to face budget challenges, struggles to gain the confidence of private-sector partners, and is involved in a large DHS reorganization of certain Chemical, Biological, Radiological, and Nuclear counterterrorism activities.

Now that Dr. Brothers is a free agent, no longer bound by OMB, I will be interested in his candid observations on these issues and how the committee can help bolster S&T's credibility as the research and development hub that drives acquisition decisions in the Department.

Mr. DONOVAN. The gentleman yields back. I thank him for his statement.

Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

NOVEMBER 7, 2017

I want to send my condolences to the families affected by last week's tragic terrorist attack in New York City and to thank the first responders for their heroic efforts.

I also want to send my thoughts and prayers to the families of those killed at the First Baptist Church in Sutherland Springs, Texas on Sunday. Over the past 5 years, we have seen mass killings at an elementary school, a movie theater, a work place, a night club, a college campus, and a music festival.

No community is immune from the indiscriminate pain that mass shootings inflict. It is time for Republican leadership to put aside politics and take meaningful

steps to ensure that this Nation's gun laws work to protect our citizens and law enforcement.

Turning to the subject of today's hearing, I am pleased that this subcommittee is continuing the committee's efforts to help S&T mature into a dynamic research and development organization capable of meeting the evolving needs of the Homeland Security Enterprise.

When the committee last held a hearing on the Science and Technology Directorate, I raised concerns about the lack of a unified DHS policy defining research and development priorities, stakeholder engagement processes, and on-going budget challenges.

I am pleased that the former under secretary for science and technology, Dr. Reggie Brothers, is here today to talk about what he did to tackle those challenges.

From identifying DHS's Visionary Goals and establishing the Integrated Product Team process to launching the Homeland Security Innovation Program, Dr. Brothers provided clarity to S&T's long-term priorities, improved the coordination of research and development activities, and attracted new industry to the homeland security space.

I commend Dr. Brothers for his efforts to leave S&T a better organization than it was when he found it.

That said, there are on-going challenges undermining S&T's potential. First, S&T's budget is not what it should be, and the Trump administration's fiscal year budget request sought irresponsible cuts that would have cut into the bone of S&T's activities.

Although I am pleased that some of the funding was restored in the House spending measure, I remain concerned that research and development of security technologies is not a top priority of the Trump administration.

Second, Congress has failed to enact legislation to clarify S&T's mission and authorities. Despite this committee's efforts to address long-standing challenges at S&T, our Senate counterparts have so far refused to act. I hope for a different outcome this Congress.

Last, I am not confident we are fully leveraging the expertise of all of the colleges and universities that are capable of contributing in this space, and I hope to learn more about how S&T can better work with academic institutions.

Before I close, I want to echo Ranking Member Payne's comments regarding the need to reschedule the full committee hearing on the Federal Emergency Management Agency's preparedness and response capabilities as soon as possible.

The Federal response to the devastation caused by hurricanes in Puerto Rico and the U.S. Virgin Islands is not what it should be, and American citizens are suffering as a result. If we can put a man on the moon and bring him back, surely we can turn the power back on and provide reliable access to clean water within 7 weeks.

Mr. DONOVAN. We are pleased to have a very distinguished panel before us today on this important topic, and I assure you all that your testimony is very important to us. This subcommittee has used testimony in every hearing that we have conducted in the last 2½ years to come up with some results, so your efforts here today will be taken into consideration, and a product will be developed from them.

Chief Timothy Rice serves as the weapons of mass destruction branch coordinator for the New York City Fire Department. He currently serves on New York City's Radiological Response and Recovery Committee, and New York City BioWatch Stakeholders Working Group.

Dr. Gerald Parker, Jr. is the associate dean for Global One Health at the College of Veterinary Medicine and Biomedical Sciences, and campus director for Global One Health at Texas A&M University. Dr. Parker also serves on several advisory boards, including the Homeland Security Science and Technology Advisory Committee, and Biodefense Blue Ribbon Panel.

Mr. Jacob Parker is the director of government relations for the Security Industries Association, and leads the development of the association's legislative and regulatory programs. Before coming to

SIA, Mr. Parker served for more than a decade on Capitol Hill, covering homeland security, defense, foreign policy and other issues.

Dr. Reginald Brothers served as the under secretary for science and technology from April 2014 to January 2017. Prior to leading S&T, Dr. Brothers served in the U.S. Department of Defense's Office of the Assistant Secretary for Defense for Research and Engineering as the deputy assistant secretary of defense for research. In this position, he was responsible for policy and oversight of the Department's science and technology programs, from basic research through the advanced technology development.

The witnesses' full statements will appear on the record, and the Chair now recognizes Chief Rice for 5 minutes.

**STATEMENT OF TIMOTHY RICE, BATTALION CHIEF, WEAPONS OF MASS DESTRUCTION BRANCH COORDINATOR, CITY OF NEW YORK FIRE DEPARTMENT**

Mr. RICE. Good morning, Chairman Donovan, Ranking Member Payne, and Members of the Subcommittee on Emergency Preparedness, Response, and Communications. My name is Battalion Chief Timothy Rice, and I am the weapons of mass destruction branch coordinator for the New York City Fire Department. Thank you for the opportunity to discuss the relationship between the FDNY and the Department of Homeland Security Science and Technology Directorate.

In May 2001, FDNY's chief of Hazardous Materials Operations, Jack Fanning, appeared and testified before Congress on the topic of Government capabilities against terrorism. Chief Fanning was one of the firefighters who responded to the World Trade Center bombing in 1993. Beginning with that attack, the role of the fire service began to shift into the area of disaster preparedness and responding to acts of terrorism. In his testimony, Chief Fanning described this shift, and he detailed some of the plans and coordination that the FDNY and Federal partners were undertaking as a result. He made it clear that those efforts were the tip of the iceberg, and that much work remained to be done.

I have seen the value of S&T in my own career. As a young firefighter in Washington Heights, I remember our fires had a radiation survey meter. It was kept in the office under the captain's bunk, and we were not sure quite how to use it. However, today we have radiation equipment on every apparatus, and every firefighter carries not just the equipment, but the competency to employ it.

As the range of threats against New Yorkers has grown and the risk of terror incidents broadens, the department continues to adapt. We confront a wide variety of challenges beyond the traditional view of firefighters running into burning buildings. As Chief Fanning put it in 2001, "At mass casualty incidents, no matter the scale, firefighters and other first responders will be there within minutes, and they will do what they have always done: Act to protect the public they serve." Knowing this, he urged Congress, "Let us provide them with the tools they need to perform their duties safely and effectively."

Four months after delivering that testimony, Chief Fanning made the ultimate sacrifice at the World Trade Center. However,

his tremendous legacy endures, as has the point that he made during that Congressional hearing. Members of the FDNY, NYPD, emergency management, and all first responder agencies are going to show up and protect the public, and we are tremendously appreciative of the ways in which our Federal partners, such as our colleagues at S&T, provide us with the tools to perform our duties safely and effectively.

For more than 15 years, the National Urban Science and Technology Laboratory, NUSTL, in New York City has been a valuable resource to the FDNY. NUSTL is our conduit to S&T, and it helps the FDNY develop capabilities necessary to provide the highest levels of security for the New York UASI region.

The scientific data, equipment testing, training, and support provided by NUSTL assist the FDNY in navigating the thousands of products, equipment, technology, and reports that we would otherwise be left to evaluate our own. We have invested heavily in all hazards and chemical, biological, radiological, and nuclear preparedness in units throughout the department, including hazmat and marine resources.

In addition to our partnerships, I must also highlight the critical importance of homeland security grants, particularly UASI, in facilitating the FDNY's ability to make many of these investments. We pride ourselves on being good stewards of those programs, and with the support of S&T, have been very successful.

NUSTL also helps to enhance the fire department's capabilities to prepare for, respond to, and mitigate potential radiological and nuclear threats. Incidents around the world like Goiania, Chernobyl, and Fukushima have all shown that radioactive contamination will lead to wide-spread public panic. By working together with our partners at S&T and the scientific community, we have been able to operationalize procedures such as the deployment of community reception centers, which will enable us to rapidly screen nearly a million people or more who may fear contamination. We have also provided input into an S&T operational guide titled "RDD Guidance for the First 100 Minutes."

The knowledge we have gained and the plans we have developed inform first responder agencies across the Nation. New York City agencies have broad outreach, and it is through these avenues that we disseminate what we have learned, gain valuable feedback, and consistently work to improve preparedness.

The NUSTL lab's location in lower Manhattan enables fire department personnel to access it with regularity. Our members attend monthly meetings for first responders, and periodic forums such as the New York Area Science and Technology Forum. NUSTL personnel also travel to fire department facilities across the city, and provide critical on-site guidance and evaluation.

Homeland security is an immense challenge, and the New York City Fire Department is in a constant state of assessing and improving our resources to meet that challenge. Through our frequent and valuable interactions with NUSTL, the FDNY has greatly benefited from our partnership with S&T. The advantages of this relationship, both tangible and intangible, strengthen the department's ability to save life and property, and ultimately, make the people of New York and millions of visitors to the region safer each day.

I thank you for your invitation to share experience with the Science and Technology Directorate, and that is the end of my statement, sir.

[The prepared statement of Mr. Rice follows:]

PREPARED STATEMENT OF TIMOTHY RICE

NOVEMBER 7, 2017

Good afternoon Chairman Donovan, Ranking Member Payne, and Members of the Subcommittee on Emergency Preparedness, Response, and Communications. My name is Battalion Chief Timothy Rice and I am the weapons of mass destruction branch coordinator for the New York City Fire Department (FDNY). Thank you for the opportunity to discuss the relationship between the FDNY and the Department of Homeland Security's Science and Technology Directorate (S&T).

In May of 2001, FDNY's Chief of Hazardous Materials Operations—Jack Fanning—appeared and testified before Congress on the topic of Government Capabilities Against Terrorism. Chief Fanning was one of the firefighters who responded to the World Trade Center bombing in 1993. Beginning with that attack, the role of the fire service began to shift into the area of disaster preparedness and responding to acts of terrorism. In his testimony, Chief Fanning described this shift and he detailed some of the plans and coordination that the FDNY and Federal partners were undertaking as a result. He made it clear that these efforts were the tip of the iceberg and that much work remained to be done.

I have seen this first-hand throughout my own career. As a young firefighter in Engine 84 in Manhattan, I remember that our firehouse had a radiation survey meter. At the time, we kept it in the office under the Captain's bunk. However, as the range of threats against New Yorkers has grown and the risk of terror incidents broadened, the Department has had to adapt. We now confront a wide variety of challenges beyond the traditional view of firefighters running into burning buildings. As Chief Fanning put it in 2001, at mass casualty incidents—no matter the scale—firefighters and other first responders will be there within minutes and they will do what they have always done: Act to protect the public they serve. Knowing this, he urged Congress, “let's provide them with the tools they need to perform their duties safely and effectively.”

Four months after delivering that testimony, Chief Fanning made the ultimate sacrifice at the World Trade Center. However, his tremendous legacy endures, as does the point that he made during that Congressional hearing. Members of the FDNY, NYPD, Emergency Management, and all first responder agencies are going to show up and protect the public, and we are tremendously appreciative of the ways in which our Federal partners such as our colleagues at S&T provide us with the tools to perform our duties safely and effectively.

It is not an easy task for a fire department to evolve from a role of traditional firefighting to a department that is also responsible for disaster preparedness, including acts of terrorism and the deliberate release of chemical and/or radiological materials and explosives. To stay ahead of emerging threats, the FDNY sought a partner in the scientific community to provide independent scientific research, data, expertise, and testing.

For more than 15 years, the National Urban Security Technology Laboratory (NUSTL) in New York City has been a valuable resource to the FDNY. NUSTL is our conduit to S&T and it helps the FDNY develop capabilities necessary to provide the highest levels of security for the New York Urban Area Security Initiative (UASI) region. The scientific data, equipment testing, training, and support provided by NUSTL assists the FDNY in navigating the thousands of products, equipment, technology, and reports that we would otherwise be left to evaluate on our own. We have invested heavily in All Hazards preparedness and chemical, biological, radiological, and nuclear (CBRN) preparedness in units throughout the Department including HazMat and Marine resources. In addition to our partnerships, I must also highlight the critical importance of Homeland Security grants—particularly UASI—in facilitating the FDNY's ability to make many of these investments. We pride ourselves on being good stewards of those programs, and with the support of S&T, we have been very successful.

NUSTL also helps to enhance the Fire Department's capabilities to prepare for, respond to, and mitigate potential radiological and nuclear threats. Incidents around the world like Goiana, Chernobyl, and Fukushima, have all shown that radioactive contamination will lead to wide-spread public panic. By working together with our partners at S&T and the scientific community, we have been able to operationalize

procedures that will greatly assist the response and recovery from incidents of this magnitude, such as the deployment of Community Reception Centers (CRCs), which will enable us to rapidly screen nearly a million people or more who may fear contamination. By performing screenings at CRCs, we will avoid flooding area hospitals and emergency rooms and preserve resources for the seriously injured, thereby saving more lives. We've also provided input to an S&T operational guide covering RDD Guidance for the First 100 Minutes.

The knowledge we have gained and the plans we have developed inform first responder agencies across the Nation. New York City agencies have broad outreach and it is through these avenues that we disseminate what we have learned, gain valuable feedback, and consistently work to improve preparedness.

To give one example, understanding the impact of a dirty bomb on the city involves understanding and predicting a number of scientific factors. Firefighters do not receive intensive training to study the physics of radiological material or to model plume clouds. NUSTL and other partners within S&T help first responders to understand the relationship between modeling and ground truth data, and they provide us with the capability to use data to better inform our radiation modeling. This allows us to respond in a more informed and effective manner. It is a collaboration that empowers the FDNY to make educated decisions about where we should set up equipment, create zones in which first responders may safely operate, and understand dangerous areas to be avoided. The Department benefits from having access to subject-matter experts in close proximity and in turn we share the knowledge and experience we have gained with first responder agencies Nation-wide.

The NUSTL lab's location in lower Manhattan enables Fire Department personnel to access it with regularity. Our members attend monthly meetings for first responders and periodic forums on CBRN preparedness and emerging threats. NUSTL hosts and manages the New York Area Science and Technology Forum, which brings together Government and private-sector resources to promote and discuss advances in science and technology. NUSTL personnel also travel to Fire Department facilities across the city to provide critical on-site guidance and evaluation. NUSTL plays a key role in the Department's preparedness and response planning for terrorist incidents, industrial accidents, and routine emergencies.

This level of on-going support and engagement with NUSTL has helped the Department build a preparedness cycle of continuous learning and training. The more we train for specific scenarios, the more prepared we are to face them when they arise.

With the help of NUSTL, the Department developed the Tiered Response System, which functions as a force-multiplier, outfitting FDNY with a mechanism to scale and adapt the appropriate expertise to the incident or emergency. We also build systems of collaboration, partnering with other city agencies and regional responders to share lessons learned and to develop interagency plans, protocols, and drills. Members of the Department have acquired a tremendous amount of knowledge and know-how since 9/11 and this knowledge is helping the city plan and prepare for extreme hazards and emergencies.

Specific NUSTL programs that FDNY participates in include:

- *Radiological/Nuclear Response and Recovery (RNRR) Research and Development*
  - This project is aimed at improving State and local response to radiological and nuclear events. FDNY and other New York-area agencies participate in working groups and coordinate to develop guidance and tools to enhance preparedness and response capabilities.
- *System Assessment and Validation for Emergency Responder (SAVER)*
  - The SAVER program provides first responder agencies with the results of NUSTL testing and assessments of commercially-available emergency response technologies. As a city agency, the SAVER program is useful for learning about the existence of new technology as well as the availability and performance of that technology. This enables us to redeploy resources that may otherwise have been consumed by the process of investigating, testing, and assessing potential advances in the market. In addition, FDNY and other New York-area agencies have the opportunity to articulate gaps and needs and receive guidance about potential solutions.
- *Critical Incident Management Technology Assessment (CIMTA)*
  - The Critical Incident Management Technology Assessment is an annual event that is staged by NUSTL in order to provide FDNY and other New York-area agencies with an opportunity to test cutting-edge first responder technologies on a large scale under real-life conditions. In the course of the event, first responder agencies are able to provide training, field-test equipment, understand the strengths and weaknesses of preparedness training, and collaborate

with technology developers to fill potential equipment gaps. Past examples have included testing handheld mobile detection and collection equipment, wide-angle thermal imaging cameras, and video content analysis and video analytics.

- *Urban Operational Experimentation (OpEx)*
  - Urban Operational Experimentation provides first responder agencies such as FDNY an opportunity to view demonstrations of innovative products and a chance to experiment with those products in an urban environment. The program brings private-sector partners in contact with first responder agencies, serving as a catalyst to allow agency feedback to spur advances in technology.
- *New York Area Science and Technology Forum (NYAST)*
  - The New York Area Science and Technology Forum convenes Federal, State, and local first responders as well as groups from academia and the private sector to meet and discuss advances in science and technology. These regular meetings bring together a wide variety of groups and lead to critical sharing and learning among the participants, helping the entire first responder community stay up-to-date on advances in the field.
- *Performance Test and Evaluation (PTEN)*
  - NUSTL's Performance Test and Evaluation program provides testing of radiation detection equipment to ensure that it works properly and that all supporting accessories and devices are functional. Performed in conjunction with the Domestic Nuclear Detection Office's Securing the Cities program, PTEN involves not only equipment testing but also provides first responder agencies with technical guidance and support and expert advice regarding storage and deployment of the devices. This includes equipment such as personal radiation detectors, backpack detectors, mobile detection units, and isotope identifiers.
- *Responder Training and Exercise (RTE)*
  - Also performed in conjunction with the Domestic Nuclear Detection Office's Securing the Cities program, NUSTL's Responder Training and Exercise program provides first responder agencies with radioactive sources, training equipment, and technical expertise to enhance training on radiation detection equipment. This includes supplying health physicists and technical staff, training equipment, and materials.

Homeland security is an immense challenge and the New York City Fire Department is in a constant state of assessing and improving our resources to meet that challenge. Through our frequent and valuable interactions with NUSTL, FDNY has greatly benefited from our partnership with S&T. The advantages of this relationship—both tangible and intangible—strengthen the Department's ability to save life and property and ultimately make the people of New York and millions of visitors to the region safer each day.

I thank you for your invitation to share our experience with the Science and Technology Directorate and I am happy to answer your questions at this time.

Mr. DONOVAN. Thank you, Chief Rice.

The Chair now recognizes Dr. Parker for 5 minutes.

**STATEMENT OF GERALD W. PARKER, JR., ASSOCIATE DEAN FOR GLOBAL ONE HEALTH, COLLEGE OF VETERINARY MEDICINE AND BIOMEDICAL SCIENCES, TEXAS A&M UNIVERSITY**

Mr. GERALD PARKER. Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee, I am honored to appear before you today to provide my perspectives on the Department of Homeland Security's Science and Technology Directorate.

The complexity and changing nature of the threats we face today, from terrorism to pandemics, are compounded by the complexity of our Nation's vast Homeland Security Enterprise that extends far beyond the Department of Homeland Security. The S&T Directorate has a critical role in helping unlock our Nation's creative imagination and innovative spirit, which is vital to defending against the known and unknown threats to homeland security. I believe our Nation's universities must be strong partners with S&T

in this effort, either through the Centers of Excellence programs, or other programs.

The S&T Directorate has made great strides since its founding, and particularly more recently, under the leadership of my panel colleague, Dr. Brothers. Dr. Brothers applied sound leadership principles that effectively brought focus to the Department's evolving near and longer-term needs. He also placed priority on the employee morale that improved the command culture of the directorate.

Although the S&T Directorate is in better shape than ever, continued evolution is essential, as the threats and challenges will evolve, too. But harnessing the broader interagency Homeland Security Science and Technology Enterprise, particularly for bio-defense, is also an important policy question.

What is the role of the S&T Directorate? To serve only the DHS components, or to help drive the broader interagency research enterprise, to include funding shared homeland security gaps that may be a primary purview of another Federal agency? Examples include defense against animal agriculture from bioterror attacks, and biological attribution.

I believe DHS/S&T interagency leadership is essential. As originally envisioned, the S&T Directorate should have assumed a larger bio-defense leadership role through biological risk assessments. But a link between risk assessments to interagency homeland security priorities and appropriations remains elusive. It is now clear this will require White House leadership coupled to a new National strategy, as recommended by the Bio-defense Blue Ribbon Panel.

The administration's pending bio-defense strategy and decisional leadership may result in renewed interest in a need to reboot the DHS/S&T risk assessments, and play a larger interagency role. A near-term concern, the President's 2018 budget request, proposed to eliminate agricultural and animal-specific homeland security research by the S&T Directorate, and has recommended closure for the National Bio-defense and Analysis Countermeasures Center, or NBACC, to provide savings for other priorities.

DHS, with substantial contributions from the State of Kansas, will spend well over \$1 billion to construct the National Bio and Agro-Defense Facility, or NBAF. The homeland security research needs of NBAF have been documented. However, NBAF will not reach its potential without Federal funding for the critical research its planners envisioned. That included USDA and DHS/S&T research programs.

Recommended closure of the NBACC also raises questions about the NBAF that is still under construction. Does the same fate await the NBAF?

These examples signaled diminished DHS and Executive branch support for agricultural biosecurity research specifically, and bio-defense in general at a time that we should elevate this issue, not push it off until next outbreak or bioterror attack, when it will be too late. The recent Ebola and avian flu outbreaks demonstrate this threat.

Beyond bio-defense, these two homeland security examples—the need for interagency leadership and adequate funding support—may be symptomatic of a larger policy issue for the S&T Direc-

torate. Is the S&T Directorate saddled with legacy laboratory infrastructure that does not fit the DHS internal priorities today, even if these assets are important to the broader enterprise? It may be better policy to transfer it to the appropriate lead Federal agency to own, operate, and maintain critical laboratory infrastructure, such as the NBAF, NBACC, or other laboratories, rather than proposed closure, or maintaining the status quo within DHS/S&T. It is a policy question.

There are many issues to consider in such a policy option where pursued, but the end result may be better stewardship of critical laboratory assets needed for the broader Homeland Security Enterprise. It may also allow the S&T Directorate to focus on a research innovation portfolio that can more easily flex to changing needs over time, and better engage university scientists.

Thank you for the opportunity to appear before you today. I will be happy to answer your questions. Thank you.

[The prepared statement of Mr. Gerald Parker follows:]

PREPARED STATEMENT OF GERALD W PARKER, JR.

NOVEMBER 7, 2017

Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee, I am honored to appear before you today for this hearing entitled, “How Effective is the Department of Homeland Security’s Science and Technology Directorate? Stakeholder Perspectives”.

As a matter of full disclosure, I am a member of the Homeland Security Science and Technology Advisory Committee (HSSTAC), but I appear before you today representing my own perspectives, and not of the HSSTAC nor Texas A&M University. I will offer insights from my role as a public servant that spanned 26 years active-duty military service primarily in Army medical research & development at the United States Army Medical Research and Materiel Command and the United States Army Medical Research Institute of Infectious Diseases; 10 years in the career senior executive service (DHS, HHS, and DOD); and now as faculty/administrator at Texas A&M University.

I do not have to tell you how difficult the homeland security mission is today. You are well aware of the challenges, and the difficult decisions that must be made regarding authorizations, budget allocation, and appropriations for the many competing demands.

The homeland security mission is extremely complex and the threats we face are constantly evolving and range from terrorism, natural disasters, and pandemics. Threats from terrorism and violent extremism include the use of weapons of mass destruction against our Nation, the civilian population, and our critical infrastructure.

Today, I am more concerned than ever about the risks from biological threats—including bioterrorism and naturally-occurring transboundary emerging infectious diseases that could affect humans, animals, and our economy. Although we are much better prepared today, partly due to the dedicated efforts of the DHS Science and Technology Directorate and many others across the vast U.S. Government inter-agency; State, local, territorial, and Tribal governments; and non-government organizations. However, recent reports by the Biodefense Blue Ribbon Panel tell us that we have a long way to go; These reports include “A National Blueprint for Biodefense: Leadership and Reform Needed to Optimize Efforts”<sup>1</sup> and “Defense of Animal Agriculture: A Report of the Biodefense Blue Ribbon Panel”<sup>2</sup>. Recent high-consequence infectious disease outbreaks, to include the Ebola outbreak of 2014–2016 and Highly Pathogenic Avian Influenza outbreaks in the United States from 2014 to 2016, also tell us we are not prepared, and remain highly vulnerable to naturally-occurring transboundary infectious diseases, as well as bioterror attacks.

<sup>1</sup>Blue Ribbon Biodefense Study Panel. *A National Blueprint for Biodefense: Leadership and Reform Needed To Optimize Efforts*. October 2015.

<sup>2</sup>Blue Ribbon Biodefense Study Panel. *Defense for Animal Agriculture*. October 2017.

I previously testified before the House Committee on Energy and Commerce's Subcommittee on Oversight and Investigation, and I will repeat a statement I made then in my testimony today:<sup>3</sup>

1. Biological threats are real, and the bioterror threat has the potential to cause mass casualties on a scale similar to a nuclear weapon;
2. The inter-epidemic period, or time between outbreaks, requires urgent action to optimize available resources and biopreparedness; and
3. Strong centralized leadership will be necessary to drive urgent action in the inter-epidemic period.

This statement has relevancy to the topic today regarding the DHS Science and Technology Directorate. We cannot afford to remain complacent about biological threats, nor can we afford to continue business as usual. Innovation, creative imagination, and leadership are more important than ever.

The complexity and changing nature of the threats we face today, including from biological threats, are confounded by the complexity of the vast homeland security enterprise. The homeland security enterprise extends far beyond the Department of Homeland Security. Other Federal department/agencies have homeland security responsibilities, as do State, local, territorial, and Tribal governments, and the private sector. I also believe that communities, families, and individuals have homeland security and preparedness responsibilities, too.

Science and Technology will play a key, if not a vital, role in defending against the many threats to homeland security. But, harnessing the interagency science and technology enterprise that extends beyond the Department of Homeland Security's Science and Technology Directorate to take urgent action on the highest priorities in a focused manner that optimizes available resources remains elusive. I am also concerned that Department of Homeland Security's Science and Technology Directorate may not give biological threats priority consideration. I am particularly concerned that the DHS Science and Technology Directorate may eliminate funding for research and development for animal agriculture defense, and that the National Biodefense and Analysis Countermeasures Center may be closed.

Finally, funding for the University Centers of Excellence is significantly reduced by the DHS Science and Technology Directorate in the President's budget request on a yearly basis only to be restored by Congress; I can understand the Science and Technology Directorate's need to have more budget discretion for research and development accounts, but if the S&T Directorate is not satisfied with the performance of the University Centers of Excellence then the whole program should be considered for elimination, rather than a slow attrition through reduced funding for the centers. That uncertainty only serves as a disincentive for university participation. However, the original intent of the Science and Technology Directorate to engage university scientists in homeland security solutions remains unchanged and should be valued and embraced by the Department rather than continually reduced in the budget exercise. I strongly recommend maintaining the University Centers of Excellence program, or an alternative strategy that maintains meaningful university involvement to ensure our best and brightest academicians are included in homeland security solutions in a manner to how the Defense Department ensures that universities are included in National security solutions.

Fortunately, the Trump administration is developing a new National strategy for Biodefense as recommended by the Biodefense Blue Ribbon Panel.<sup>4</sup> Although the new strategy has not been released, I am hopeful that the biodefense strategy will be comprehensive, and include strategies for the defense against attacks, outbreaks, and accidents; linked to a unified interagency budget; and include strong White House leadership with clearly-identified lead and supporting accountability metrics for all Departments and Agencies, including the Department of Homeland Security and the underpinning Science and Technology Directorate.

Interagency coordination and leadership for the homeland security science and technology enterprise is an important policy question that hopefully will be addressed in the new National strategy. The strategy should include a clearly-identified role for the Department of Homeland Security (DHS) Science and Technology Directorate.

Regarding the primary question for this hearing, I believe the Department of Homeland Security's Science and Technology Directorate has made great strides since its establishment by the original homeland security act, and particularly in

<sup>3</sup> Gerald W Parker, Jr., DVM PhD. Hearing of the House Committee on Energy and Commerce Subcommittee on Oversight and Investigations. *Attacks, Outbreaks and Attacks*. February 12, 2016.

<sup>4</sup> Blue Ribbon Biodefense Study Panel. *A National Blueprint for Biodefense: Leadership and Reform Needed To Optimize Efforts*. October 2015.

recent years under the leadership of Dr. Brothers and Dr. O’Toole. Dr. Brothers established new, visionary goals and areas of focus that included: (1) Responder of the future; (2) Enabled decision makers; (3) Screening at speed; (4) Trusted Cyber Future; (5) Transformed airport borders; (6) Resilient communities; and (7) CBRN defense. Dr. Brothers also extended the APEX Program initiated by Dr. O’Toole, and brought a sense of priority to meeting near-term requirements of the Department of Homeland Security components over those needs of the broader homeland security enterprise. Command culture and worker satisfaction of the Science and Technology Directorate also made great strides during Dr. Brother’s tenure as the under secretary. I know several program managers and scientists in the Science and Technology Directorate. They are dedicated professionals working hard to make a difference, and I believe they are making a difference.

Performing organizations supported or funded by the Science and Technology Directorate—whether from National laboratories, universities, and the private sector—are also making a difference, and I believe largely enjoy the working relationship they have with the Science and Technology Directorate. However, I also believe the uncertainty of not having a new under secretary for the Directorate is causing apprehension for the Directorate’s staff and performing organizations. It is critical that a new under secretary be appointed and approved soon.

Despite the hard work by many and the progress to date, I believe the Science and Technology Directorate has ceded responsibility to be a lead coordinator for the broader science and technology homeland security enterprise. I believe an interagency lead role for the broader homeland security enterprise is required as originally envisioned when the DHS Science and Technology Directorate was established—particularly for biodefense. It is clear now that strong leadership for the interagency biodefense enterprise is needed now more than ever before.

To provide context, I joined the Department of Homeland Security’s Science and Technology Directorate in 2004. There was a true sense of urgency at that time as the Directorate was established after the terrorist’s attacks on September 11, 2001, the anthrax letter attacks a few weeks later, enactment of Project BioShield, and issuance of Homeland Presidential Directives 9 and 10. The Science and Technology Directorate placed high priority on defense against weapons of mass destruction—including biological threats—and assumed an interagency leadership role for the homeland security scientific enterprise. Biodefense threat, risk, and net assessments were established with the intent to drive interagency requirements and provide leadership for biodefense programs across the interagency. The National Security Council and Office of Science and Technology Policy also provided effective White House-level policy leadership that relied on early DHS risk assessments. Initial attempts by DHS S&T to lead, coordinate, and fund, where appropriate, the broader science and technology homeland security enterprise were initially successful. However, over time it became clear that other agencies were not receptive to being “coordinated” by DHS S&T. In defense of the interagency, the style of leadership practiced by DHS S&T as time went on was not as collegial and transparent as it could have been for success.

Today, I see a Science and Technology Directorate that is more concerned with staying in their “lane” and serving only the DHS components as more important than playing a broader homeland security enterprise leadership coordinating role. I also see a broader interagency homeland security enterprise that does not place value on the DHS threat and risk assessments in driving their own homeland security requirements. From what I can discern, DHS S&T seems to have also abandoned their practice of conducting interagency biodefense net assessments, too.

In defense of the S&T Directorate, competing and “siloed” interagency biodefense interests are now common-place, leading to a relative lack of interagency coordination and inefficient use of available resources for the growing biological threats.<sup>5</sup> Departmental and Congressional pressures have also led to an inward, DHS-only component focus. These issues only highlight the critical importance for a new biodefense strategy and renewed strong White House leadership for Biodefense.

There are two other concerns of the DHS Science and Technology Directorate that I will highlight in my testimony. Defense of Animal Agriculture and Biological Attribution.

The Department of Homeland Security Science and Technology Director assumed operations for the Plum Island Animal Disease Laboratory and has embarked on an aggressive construction campaign to move those unique large animal research and defense functions from Plum Island in New York to the National Bio and Agro-Defense Facility (NBAF) at Kansas State University in Manhattan, Kansas. Construc-

<sup>5</sup> Blue Ribbon Biodefense Study Panel. *A National Blueprint for Biodefense: Leadership and Reform Needed To Optimize Efforts*. October 2015.

tion is well under way and promises to provide a state-of-the-art facility to enable critical animal health and biodefense research. The DHS S&T Directorate also supported critical research and development funding for defense against agriculture bioterrorism that is filling critical gaps identified by USDA and other key homeland security stakeholders that otherwise would not have been funded by USDA.

The President's 2018 budget request eliminates DHS Science and Technology funding for animal agriculture bioterrorism defense. This is a concern not only of mine, but several animal health stakeholders, that include State veterinarians, as well as animal health and production industries that have homeland security responsibilities. As a policy option, there is merit to shifting DHS S&T requirements and funding to USDA under existing USDA authorities and appropriations. If this is done, DHS S&T should also consider transferring the NBAF to USDA. But it is not apparent that DHS research and development requirements and programs have been coordinated with USDA for an effective transition. Rather, it appears that ongoing research and development programs supported by DHS S&T for agriculture bioterrorism defense will be terminated. This will not only cause a research and development gap, but it also causes uncertainty for the business and operations model envisioned for the NBAF, as well as on-going commitments to the importance, or not, of defense against agriculture bioterrorism. Time will tell if the new biodefense strategy and Congressional intent will address this gap. It is hoped that the new National biodefense strategy will incorporate the recommendations of the Biodefense Blue Ribbon Panel on issues related to animal health, and incorporate the practice of one health into that strategy. If not, the business and operations model of the NBAF could be in jeopardy, as well as our capability to conduct research and diagnostics for high-consequence foreign animal diseases. I hope that latter is not the case as it could be a costly mistake to our economy and well-being in the long run.

The President's DHS S&T budget request for fiscal year also eliminates funding that would force closure of a state-of-the-art, one-of-a-kind biocontainment laboratory—the National Biological Analysis and Countermeasures Center (NBACC) at Fort Detrick, MD. This decision seems short-sighted and not well-considered.

Naturally-occurring and man-made biological threats pose a grave risk to our health and National security. Globalization, population growth, urbanization, and other factors are creating a perfect storm for the emergence of high-consequence infectious diseases. A terrorism nexus also exists in many of these same global disease "hot spots", and together, are changing the nature of biological risks.

This is exacerbated by the diffusion of technical expertise coupled with the biotechnology revolution, drastically increasing the threat of bioterrorism. New technologies have decreased resources and financial requirements for entry, and increased capabilities that could be misused by a determined bioterrorist.

There are many that believe we need to strengthen infectious disease surveillance and laboratory capabilities to detect threats early—an area that DHS also plays a role. Similarly, we need core microbial forensic laboratory capabilities to enable attribution—an area that DHS has a primary role.

As stated earlier in my testimony, I am more concerned than ever about the risk of biological threats—whether from outbreaks, accidents, or attacks. This includes a need to underpin no-regret attribution decisions with a sound scientific foundation in microbial forensics.

The anthrax letter attacks marked the first significant act of bioterrorism in the United States. That attack was one of the easiest bioterror attacks to confront, yet the impact was far-reaching. As bad as it was, it could have been much worse had the pathogen involved been a contagious agent, resistant to antibiotics, an unknown pathogen, or delivered in a covert wide-spread aerosol attack across multiple jurisdictions. As it was, the anthrax letters shut down the Hart Senate Office Building for 3 months, wreaked havoc with the U.S. Postal Service, reduced business productivity, cost the Nation more than \$1 billion, and tragically, took 5 lives and sickened 17 more. More than 30,000 people required post-exposure antibiotics.

Many still recall frightening moments experienced during that time, particularly those who were potentially exposed to anthrax spores in the Hart Senate Office Building, postal processing facilities, and media offices.

This event also forever changed our notions of laboratory biosecurity, biosafety, and personal reliability in the biological sciences, and the emerging science of microbial forensics. An understanding of the importance of microbial forensics was greatly accelerated at that time. I, along with many others at the FBI and in the DHS Science and Technology Directorate were involved in defining the laboratory requirements needed to support a core capability for microbial forensics. Unfortunately, decisions being made today regarding the NBACC seem to have lost our lessons learned from first-hand experience during that era.

The follow-on FBI Anthrax investigation applied the emerging science of microbial forensics, and along with traditional investigative procedures, ultimately attributed the attack to a lone U.S. scientist.

Attribution to determine who is responsible for an attack, whether a crime, act of terror, or warfare is essential to hold those responsible accountable for their actions, prevent future attacks, and serve as a deterrent. Attribution and the supporting microbial forensic sciences are also important to exonerate—and rule out—suspected perpetrators, whether a nation-state, terror group, or criminal that is innocent.

The stakes could be very high, particularly when a nation-state is involved or suspected—and a rush to judgment before the science and evidence are in, should be avoided. Decisions to attribute, especially a nation-state, will be consequential, no-regret decisions—that must be guided by a strong scientific and evidentiary foundation.

It is similarly important to differentiate a naturally-occurring infectious diseases outbreak from an attack. It may not be readily apparent that an outbreak was natural or due to an intentional cause at the first sign of disease—or even after an outbreak has run its course—whether in people or animals.

Prior to 9/11 and the anthrax letter attacks, scientists and operators from the FBI, CDC, and DOD had already begun establishing needed protocols to enable collaboration to account for public health and law enforcement requirements for sample collection and analysis, and imitated what we know today as the science of microbial forensics.

This same group also began planning for unique laboratory capabilities and the scientists that would be needed to support attribution—whether for an attack, accident, or outbreak—and to uncover and document illicit proliferation activities. The facilities envisioned then and soon after the anthrax attacks include the laboratory that was subsequently constructed and in use today at Fort Detrick—The National Biodefense Analysis and Countermeasures Center, or NBACC.

I cannot overstate the importance of having dedicated, core laboratory capabilities and scientists that are focused on microbial forensics to support attribution. It is not a part-time job, or other-duties-as-assigned function.

Microbial forensics is still, and will always be an evolving science—perhaps not well understood outside of the relatively few professionals in their field. But, prosecutors and National command authorities who will one day be thrust into the position of making no-regret attribution decisions will quickly grasp the importance of microbial forensics as essential to underpin their pending difficult decisions.

The science of microbial forensics will only get more complex with the continued rapid advancement of new biotechnology tools that are readily available, and as new examples of dual use research of concern emerge from our scientific enterprise that could be misused to do harm. A recent example is the report by Canadian scientists on the synthesis of the horse pox virus.

There was considerable thought that went into the establishment of the NBACC laboratory to support law enforcement and National security attribution. To my knowledge, those original planning assumptions have not substantially changed. I strongly recommend that those strategies and needed capabilities are not abandoned.

Finally, it is important to reiterate that the DHS Science and Technology Directorate has made great strides; the Directorate's program managers, scientist, and their contract performers are doing everything in their power to help keep our homeland safe and secure. But, we must acknowledge that the DHS Science and Technology Directorate has a difficult task. Budget limitations and other pressures will not allow them to satisfy all competing needs of the vast homeland security enterprise, not to mention those needs of just the DHS components. Given that, the Science and Technology Directorate should focus available resources on those programs that only the Federal Government must do, and address threats that are more existential in nature that the private sector cannot or will not be able to address. Biological threats, and other weapons of mass destruction largely fit this category. The Directorate should also take a longer-term view and imbed creative imagination, innovation, university scientist, and sound leadership practices in their programs. A true DARPA-type approach as originally envisioned for HSARPA is needed. Business as usual will not get the job done.

Recommendations:

1. The committee should ensure that the administration develops a comprehensive biodefense strategy that is tied to a unified and transparent budget, with clearly-identified lead and supporting roles—and support a strong White House leadership role to elevate the importance of biodefense to homeland security and drive interagency coordination and optimal use of available resources.

2. The committee should ensure that the DHS Science and Technology Directorate reestablishes leadership role in the new National strategy to help drive broader homeland security biodefense and homeland security requirements through a transparent and trusted bio-risk threat assessment and net assessment process that White House leadership can use to enforce interagency outcomes, performance, and accountability.

3. The committee should ensure the DHS Science and Technology Directorate does not eliminate their animal agriculture bioterrorism defense research and development programs unless there is a plan in place to transition those R&D requirements and programs to USDA. The committee should also work with DHS and USDA to also consider transferring NBAF to USDA if DHS does not maintain animal defense R&D programs.

4. The committee should work with the DHS Science and Technology Directorate to ensure that the National Biodefense and Analysis and Countermeasures Laboratory is not closed and to ensure that a plan for transition of ownership and operations of the laboratory to either the FBI, DOD, or the intelligence community is completed and implemented.

5. The DHS S&T Directorate and the broader DHS department should implement recommendations of the Biodefense Blue Ribbon Report.<sup>6 7</sup>

6. The DHS S&T Directorate should ensure that there is an effective mechanism to keep university scientists engaged on homeland security solutions, whether that is sustainment of the Centers of Excellence model or an alternate strategy.

7. The DHS S&T Directorate should continue implementing a more innovative, DARPA-type culture for the homeland security science and technology enterprise.

Thank you for the opportunity to appear before the hearing of the U.S. House of Representatives Committee on Homeland Security's Subcommittee on Emergency Preparedness, Response, and Communications today.

Mr. DONOVAN. Thank you, Dr. Parker.

The Chair now recognizes Mr. Parker for 5 minutes.

**STATEMENT OF JAKE PARKER, DIRECTOR OF GOVERNMENT RELATIONS, SECURITY INDUSTRY ASSOCIATION**

Mr. JAKE PARKER. Good morning, Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee. I am Jake Parker, director of government relations for the Security Industry Association, which represents nearly 800 companies that provide security technology solutions.

Thanks for the opportunity to speak about the important partnership between DHS S&T and its stakeholders in the private sector. The input I am providing here is based broadly on the experiences and perspectives that SIA member companies have shared with me, including both small and large businesses. I have tried to summarize these for you, and provide an unfiltered way as possible.

Technology provided by our industry plays a key role in DHS component operations in protecting critical infrastructure. Since November, this month, is Critical Infrastructure Security and Resilience Month, I first wanted to highlight S&T's work through the Support Anti-terrorism by Fostering Effective Technologies Act, known as the SAFETY Act. This is the most common interface between our member companies and S&T.

As you know, the SAFETY Act was passed in the aftermath of the September 11 attacks to establish a way to encourage the development and deployment of security technologies to protect crit-

<sup>6</sup>Blue Ribbon Biodefense Study Panel. *A National Blueprint for Biodefense: Leadership and Reform Needed To Optimize Efforts*. October 2015.

<sup>7</sup>Blue Ribbon Biodefense Study Panel. *Defense for Animal Agriculture*. October 2017.

ical infrastructure, and the vast majority of that infrastructure is owned and operated by the private sector. It provides liability protections for certified suppliers and end-users against claims arising from terrorist attacks, which this has been identified as a major obstacle to the deployment of the effective security measures at that time.

Not only does the SAFETY Act provide liability protections, but the designation and certification provides assurances that a product or system meets high standards of safety and effectiveness, and that it works as intended. Our industry provides manufactured products, as well as systems integration services, and even software, such as cybersecurity programs. All of these are potentially eligible, but more recently, owners and operators of facilities, such as sports stadiums, are making use of the SAFETY Act designation for their entire system of security measures as a comprehensive program, and in this, our security technology plays a key role as well.

So over the past year, we understand that 91 applications were approved by the SAFETY Act Office out of 133 submitted, taking an average of nearly 4 months to get through the process, and this has a significant jobs and economic impact. The office projected that the approval of these technologies will support 87,000 jobs, and greatly increase local business revenue.

So we believe that Congress should work to ensure this important program continues to be successful, and is provided with the resources necessary to meet the demand. Specifically, we believe that Congress should provide the SAFETY Act Office with a line item appropriation. This will provide budgetary certainty and program continuity, as well as help measure the return on investment.

On the broader array of S&T programs, we are encouraged with the recent signs the directorate is strengthening its efforts to coordinate research across DHS components and industry stakeholders.

Two years ago, when Dr. Brothers, who we are honored to have with us here today, was serving as under secretary, the integrated product teams were reestablished to track and harmonize Department-wide research and development efforts, which the Chairman highlighted was a step in the right direction, which we agree with. The most recent IPT report is only the second since this data has begun to be gathered, and a new process has been implemented for involving the operational components and identifying the gaps where S&T efforts will be the most effective. According to this most recent report, IPT's are intended to sustain a year-round process in which a specific component is designated to shepherd the process for each gap that is identified, from the point it is identified to the transition to solutions that close it.

We think this is really encouraging, because in the view of our member companies, the business case for involvement in S&T programs would be much stronger if each effort was championed by a DHS operational component that is involved at some level from the beginning of the process, and committed to making use of the technologies explored. This may result from the fact that there is a perception out there that the S&T programs only infrequently impact the operational procurement activities of DHS components

in a significant way. More involvement from the components up front could help improve this perception, as well as efforts to increase industry awareness of these new initiatives by S&T, which are more focused.

So in October, S&T released a new industry guide which I think does a great job at providing industry with the road map, teaching the ways they can participate, and summarizes the directorate's current and future needs. We understand this is the first step toward providing a centralized on-line interface for industry.

Members also tell us that for many smaller companies, responding to the call for proposals needs to be aligned with something they are already doing in order to help justify the use of resources to apply. This is especially true if the responding to grant proposals and other research opportunities is not a normal and significant part of a technology company's business model. Whether large or small, though, companies tell us that it would benefit them greatly if the process of working with S&T was easier and less bureaucratic.

We are optimistic about plans to update and improve S&T's long-range broad agency announcements process, which is sustaining requests to the private sector to develop needed technology, and it is available for funding over multi-year periods.

We understand that early next year, S&T is planning to make significant changes to this process, based on industry feedback, as it is retooled for 2019 and beyond. This includes a more direct linkage to component needs, administrative simplification, shortened review times, and clarification of a streamlined application process, and actually, an involvement from program managers prior to submission to make sure that there is the highest quality.

When it comes to the S&T research and divestment outlook for the next 4 years, the security industry is poised to contribute significantly, particularly when it comes to areas like biometrics collection and utilization, robotics and autonomous systems, enhanced situational awareness, identity credentialing and access management, automated vetting, and other technologies.

We applaud S&T's goals, outlining its 2017 innovation strategy to ensure the industry is fully engaged in meeting the demands of the Homeland Security Enterprise, and that the end-users of homeland security technology in both the public and private sectors have access to the best available products.

So we are committed to doing our part as an association to help engage industry with this effort, and look forward to answering any questions you may have. I will do my best, but if I can't, I will definitely go back to our members and provide you an answer. Thank you.

[The prepared statement of Mr. Jake Parker follows:]

PREPARED STATEMENT OF JAKE PARKER

NOVEMBER 7, 2017

Good morning Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee. I am Jake Parker, director of government relations for the Security Industry Association, a non-profit international trade association representing nearly 800 companies that develop, manufacture, and integrate security solutions, and employ thousands of technology leaders.

Thank you for the opportunity to testify before you today on the partnership between the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and its stakeholders in the private sector. The input I am providing is based, broadly, on the experiences and perspectives SIA member companies have shared with me, which include both small companies and large corporations.

Technology provided by the security industry plays a key role in DHS component operations, and in protecting critical infrastructure such as chemical facilities, airports, seaports, mass transit systems, the energy sector, Federal offices, and even K-12 schools and universities.

Since November is Critical Infrastructure Security and Resilience Month, I want to first highlight S&T's work through the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Office, which is the most common interface between SIA member companies and the Directorate. As you know, the SAFETY Act of 2002 established a process to encourage the development and wide-spread deployment of security technologies addressing the terrorist threat by providing liability protections for qualified providers against claims arising from terrorist attacks. The potential for such claims was identified as major obstacle to the deployment of effective security solutions following the attacks of September 11.

From our point of view, the program has been a major success and a catalyst for adoption of new technology in many ways. The private sector owns and operates the vast majority of critical infrastructure in the United States. Not only does the SAFETY Act protect these end-users from liability for deploying technology, SAFETY Act designation and certification provides a level of assurance that a product or system meets high standards of safety and effectiveness, and works as intended.

Our industry provides manufactured products, and well as systems integration services and software such as cybersecurity programs—all of which are potentially eligible for SAFETY Act designation or certification. In addition, owners or operators of critical infrastructure are making increasing use of the SAFETY Act designation for their comprehensive security programs, in which security technology plays a key role.

According to the SAFETY Act Office, during fiscal year 2017, 91 applications were approved out of 133 submitted, taking an average of nearly 4 months to get through the process. The Office projects that approval of these technologies will support 87,000 jobs and significantly increase revenue for providers.

We believe that Congress should work to ensure this important program continues, and importantly, is provided with the resources necessary to meet demand. Specifically, Congress should provide the SAFETY Act Office with a line item appropriation. This will provide budgetary certainty and program continuity, as well as help measure the return on investment.

As far as the broader array of S&T programs, we are encouraged with recent signs the Directorate is strengthening efforts to better coordinate research and development (R&D) activities across DHS components and with industry stakeholders. Two years ago, when Dr. Brothers—who we are honored to have with us here today—was serving as under secretary, Integrated Product Teams (IPTs) were re-established to track and harmonize Department-wide research and development efforts between S&T and the components. The most recent IPT report for fiscal year is based upon only the second round of data gathering across DHS components, as well as a new process for involving operational components in the identification of capability gaps on which to focus R&D efforts. IPTs are aimed at sustaining a year-round process in which a designated component “shepherds each gap from the identification of needs to the transition of solutions to close the gap” according to the report.

In gathering feedback from our member companies, a recurring theme was the importance of bolstering the business case for participation in S&T programs. Our members tell us that for S&T programs to be truly successful from their standpoint, each effort needs to be championed by a DHS operational component, and accompanied by some form of commitment to make use of the technologies being explored if the Government is the intended end-user. The component should have some level of involvement in the project being executed from the beginning of the process, and prior to making any significant expenditures.

There is a perception among some in the industry that S&T programs only infrequently significantly impact the operational or procurement activities of the DHS components, even with a successful engagement. For this reason, the choice may be made to devote more time and resources to focus primarily on relationships with the program offices on the component side.

More involvement from the components up front could help address this perception, as well as efforts to increase industry awareness of S&T's new initiatives. Last month, S&T released its new Industry Guide, which very effectively summarizes

current needs and programing, providing a future R&D outlook and linking industry to each of the ways to participate. We understand from discussions with personnel at S&T that they are working toward a providing a centralized on-line interface for industry to pull together information about opportunities that is currently listed in disparate locations.

Successful engagement with industry also depends on the business model of companies that possess the expertise S&T is seeking. For many smaller companies, the topic often needs to be aligned with something they are already doing to justify the use of resources to apply, especially those with limited experience with grant proposals and similar processes. S&T should do everything possible to simplify and streamline the process to make it easier for companies that do not have this expertise to participate.

Whether large companies or small, industry would benefit from making the process of working with S&T easier and less bureaucratic. This is one reason we are optimistic about plans to update and improve S&T's Long-Range Broad Agency Announcements (LRBAA) process. We understand that early next year S&T is planning to make significant changes to the process based on in industry feedback, as LRBAA's are initiated for 2019 and beyond. This includes a clarification of priorities that are linked directly to component needs, a simplified and streamlined application process, increased communications with program managers prior to submission, shortened review time as well as feedback to submitters. This feedback is particularly important for accepted proposals that are unfunded, to increase the chance of success with future submissions. Further, we think the evaluation process can be improved to the extent it can be aided by personnel with product development experience.

As you know, the Government is challenged by the fact that technology is now evolving so quickly that it often outpaces traditional Government R&D and acquisition vehicles. Meanwhile, technology-based solutions are more important than ever to achieving DHS component missions. According to the 2017 S&T Innovation Strategy, among the Directorate's goals are to ensure that industry applies its resources toward meeting the demands of the Homeland Security Enterprise (HSE), as well as to ensure that technology end-users are more satisfied with products available on the commercial market.

When it comes to the S&T R&D investment outlook for the next 4 years, the security industry is poised to contribute significantly, particularly when it comes to priority areas like biometrics collection and utilization, robotics and autonomous systems, enhanced situational awareness, identity credentialing and access management, automated vetting and other technologies.

SIA and S&T have maintained a memorandum of understanding (MOU) that facilitates information sharing on the adaptation of electronics-related technological innovation for use at the Federal, State, and local level for homeland security applications. SIA is committed to continuing to do our part to facilitate the participation of our industry in helping meet HSE needs, and we look forward to working with S&T in new and more effective ways in the future as new leadership is appointed.

On behalf of the Security Industry Association, I appreciate the opportunity to provide collective input from our industry on working with S&T. I will do my best to answer any questions you may have, however if there is any information requested I cannot provide today, I will be happy to work with our members to provide helpful responses.

Mr. DONOVAN. Thank you, Mr. Parker.

The Chair now recognizes Dr. Brothers for 5 minutes.

**STATEMENT OF REGINALD BROTHERS, PRINCIPAL, THE  
CHERTOFF GROUP, LLC, TESTIFYING AS FORMER UNDER  
SECRETARY, SCIENCE AND TECHNOLOGY DIRECTORATE,  
U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. BROTHERS. Good morning, Chairman Donovan, and Ranking Member Payne, and distinguished Members of the committee. Thank you for the opportunity to testify before you today on the role and effectiveness of the Department of Homeland Security Science and Technology Directorate.

We are now living in a post-industrial age with a globally interconnected web leading to a highly integrated world with supply chains that reach thousands of miles. Things that were previously

done only by nation-states are now accomplished by sub-state actors, gangs, groups, and even individuals. Our new reality is an asymmetric threat environment, where individuals attack government institutions, and nation-states attack civilian infrastructure with little fear of retaliation, or even attribution.

In the past, we discussed precision targeting of kinetic weapons. We are now discussing precision targeting of individuals and content on Facebook.

Technology continues to accelerate with artificial intelligence, the internet of things, commercial drones, synthetic biology and quantum computing, all promising tremendous benefits to society, but also the potential to create complex and vulnerable threat surfaces. This global threat context informs us that the Nation needs its efficiently and consistently funded agile, adaptive, and relevant and rapid innovation engine to confront the current and future threats to our National security.

DHS S&T has worked hard to focus on being highly relevant, shifting from the past focus on long-term basic research to near-term operational impact. S&T can now be an important asset for the Secretary as one of the few cross-departmental entities. S&T create a laboratory as a Department-wide resource for leading-edge data analytic and machine-learning software, where operational personnel work with S&T staff to evaluate and co-develop mission-centric solutions.

This capability resulted in a tool, using advanced facial recognition that identified 475 child sex victims, leading to their rescue from abusers.

In partnership with the New York Police Department and Metropolitan Transportation Authority, S&T installed a permanent test bed in New York City's Grand Central Terminal, an extension of our pilot demonstrations that successfully measured and mapped how and where a bioagent would be transported in the event of a terrorist attack in the subway system.

S&T completed a Tucson border security operational exercise for Customs and Border Protection and ICE to evaluate border security technology capabilities, looking at Border Patrol, HIS, and industry.

S&T also provided support of the response and recovery efforts from hurricanes Irma and Harvey with training, decision support software, and communications equipment.

Starting in December 2015, S&T initiated the Silicon Valley Innovation Program as an effort to engage creative technologists from across the world in solving pressing problems in National security. At the present time, an awareness has been built with more than 1,000 start-ups, accelerators, and venture capitalists. Six topic calls have been published, ranging from internet of things security to airport passenger processing. Applications have been received from across the country and from the international community. To date, there have been nine Phase 1 awards, and four Phase 2 awards, with the average time to award being only 45 days.

For operational relevance, collaboration with users and industry is essential. The Cybersecurity Division has developed specific and relevant industry collaborations with the energy, financial, and automotive sectors.

With the initiatives discussed above, S&T is demonstrating that it is working toward being the agile, adaptive, and rapid innovation engine I described. That said, there is a second context to consider when evaluating the potential of S&T to be effective. That second context is funding.

If the fiscal year 2018 budget cuts were to remain in effect, there would be severe impacts to the ability of DHS S&T to do its job. For example, these budget cuts would reduce the funding of the Cyber Security Division by 20 percent, the Chemical Biological Division by approximately 60 percent.

Cybersecurity is a challenge that is exponentially increasing with time. Observed malware has increased 40 times in the past 10 years. Observed attacks on critical infrastructure have increased 1.5 times in just the past 3 years. With the emergence of the internet of things, autonomous vehicles, and other networked innovations, the threat surface of our National security are rapidly expanding.

While awareness of the need for cybersecurity is increasing, the same is not necessarily true for chemical and biological security. Threats from chemical and biological threat agents, known and yet-unknown synthetic variations are real, and becoming more attractive to terrorist organizations. The National Biodefense Analysis and Countermeasures Centers, NBACC, and Chemical Security Analysis Center, CSAC, are recognized within the United States as the Nation's focal points for biological and chemical defense awareness and response. But the funding for these centers is threatened to be cut due to the fiscal year 2018 budget pressures, as well as the National Urban Security Technology Laboratory.

Given the threats to National security that our current global context mandates, I am very concerned about the impact of these potential budget cuts. From my personal experience, I know that one of the most disruptive forces for technologists and innovation organization is uncertain and unstable funding. This challenge is magnified at DHS, because a threat environment can change on a frequent basis, which can call for rapid change of investment across the R&D portfolio to meet an immediate or near-term threat.

However, while I am concerned, I also believe with the appropriate support of the Department and Congress, S&T can meet the challenges of the 21st Century.

Thank you for the opportunity to be here, and I look forward to your questions.

[The prepared statement of Mr. Brothers follows:]

PREPARED STATEMENT OF REGINALD BROTHERS

NOVEMBER 7, 2017

Good morning Chairman Donovan, Ranking Member Payne, and distinguished Members of the committee. Thank you for the opportunity to testify before you today on the role and effectiveness of 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. Having served in both the Departments of Defense and Homeland Security in senior leadership positions in science and technology, I'd like to start by giving my thoughts on the current and future threat environment as a way of providing context for the work of S&T.

We are now in a post-industrial age, with a global interconnected web leading to a highly integrated world with supply chains that reach thousands of miles. Things that previously were done only by nation-states are now accomplishable by sub-state actors, gangs, groups, and even individuals.

For the period of the Cold War, it was possible to develop strategic nuclear weapons, stealth platforms and precision weaponry and retain a competitive advantage for a decade or more. However, with the hyper-connectedness of our world and the subsequent democratization of technology, it is no longer possible to develop technology-based capabilities for National security that have any significant temporal advantage. The power to inflict harm is no longer based solely with nation-states. Our new reality is an asymmetric threat environment where individuals attack government institutions and nation-states attack civilian infrastructures with little fear of retaliation or even attribution. With easily accessible technologies such as cyber tools, drones, and potentially bio-weapons, it is possible for individuals to cause significant financial and physical damage as well as endanger human life. While we are used to discussions of precision targeting of kinetic weapons, we are now discussing precision targeting of individuals and content on Facebook. And technology continues to accelerate with artificial intelligence, the internet of things, commercial drones and satellite constellations, synthetic biology, blockchain and quantum computing all promising tremendous benefits to society but with also the potential to create devastating threat vectors and complex and vulnerable threat surfaces.

What this context tells us is that the nation needs a sufficiently and consistently funded, agile, adaptive, relevant, and rapid innovation engine to confront the current and future threats to our National security. DHS S&T has worked hard to focus on being highly relevant—shifting from the past focus on long-term basic research to near-term operational impact. I think S&T is now an important asset for the Secretary as one of the few cross-Departmental entities. I'd like to now provide a few examples.

DHS S&T created the Data Analytics Engine (DA-E) which is a Department-wide resource for leading-edge data analytic and machine learning technologies applied to Homeland Security mission sets. A laboratory has been developed where operational personnel can work with S&T staff to evaluate and co-develop technological solutions. Using this capability S&T helped NPPD deploy a social media capability to monitor publicly-available posts regarding critical infrastructure and public health. S&T delivered over 370 requests for help to emergency responders. The S&T DA-E provided solutions using advanced facial recognition tools that identified 475 child sex trafficking victims, leading to their rescue from abusers.

At the direct request of the NYPD, conducted further experiments in identifying and characterizing live streaming social media sources that are affiliated with terrorist or other criminal activity. In addition, outside of New York, S&T will evaluate an even more extensive selection of social media analytical tools on behalf of I&A, CIS, and CBP for screening and vetting to detect, characterize, and locate source(s) of content of interest on social media platforms like Periscope and Facebook Live.

In partnership with the New York Police Department and Metropolitan Transportation Authority (MTA), S&T installed a “permanent” testbed in New York City's Grand Central Terminal, an extension of S&T's pilot demonstrations successfully measuring and mapping how and where a bioagent would be transported in the event of a terrorist attack in the subway system.

On behalf of TSA, S&T conducted three live-fire exercises to better understand Home Made Explosives (HME) capabilities and impacts on critical infrastructure.

S&T completed the SkyNet Field Experiment, a Tucson Border Security Operational Exercise for CBP and ICE to evaluate border security technology capabilities linking Border Patrol, HIS, and industry. This field exercise will be used to further develop and deploy tactical data and video from Border Patrol sensors and Small UAS platforms. S&T developed sensors for Field Agents at the Tactical Operations Center, the Border Patrol eGIS system, and remote locations such as the Air Marine Operations Center. The FE was a series of scenarios centered on illegal entry by walkers, vehicles, and air platforms such as ULAs (Ultra Light Aircraft) in a Southern Border environment.

S&T finalized the stand-up of the Common DHS UAS Test Site for use by S&T, FEMA, Coast Guard, CBP, and Secret Service for testing and training on UAS technologies. Unlike the counter UAS program this test site will allow for development of UAS technologies by DHS operational components. In addition, S&T will finalize counter UAS agreements with DOD to consolidate all UAS threat databases and libraries under the JIDO umbrella.

S&T deployed the Counter Small Unmanned Aerial System (C-UAS) Advisory and Review Toolkit (C-SMART) to the Secret Service. C-SMART is a suite of computer models, databases, and analysis tools to analyze and plan C-UAS security

postures for specific operations—this capability has helped Homeland Security Enterprise (HSE) partners understand the C-UAS threat, and optimize security posture plans. C-SMART has been used in direct support of National Special Security (NSSE) and Special Event Assessment Rating (SEAR) identified events, such as the Inauguration and the Super Bowl.

S&T deployed the Next Generation Incident Command Center (NICS) to even more emergency operational centers across the Nation and world. NICS is a web-based communication platform that enables responders on scene to share data and information using open standards, and request and receive assistance from remote experts in real-time. Developed in collaboration with MIT Lincoln Labs and the Coast Guard, S&T's NICS is in use by Coast Guard assets, Cal Fire, California OES, State of Victoria Australia, and NATO member and partner countries as part of NATO's Science for Peace and Security Project Advanced Regional Civil Emergency Coordination Pilot. S&T received funding from Australia and NATO for further development of this platform. S&T has made NICS available on GitHub, the world's leading software development platform.

S&T transitioned the National Hurricane Program Technology Modernization HURREVAC-eXtended (HVX) to FEMA. HVX enables emergency managers to visualize hurricane risks associated with their specific evacuation zones, resulting in reliable and better-informed evacuation decisions. Two major improvements for HVX include providing a web-enabled system to make training widely available to emergency managers on-line, as well as accessible via mobile phone—a FEMA requirement. The initial HVX Beta will complete its transition in May 2017. Once fully operational at FEMA in 2018, substantial savings are expected by avoiding unnecessary “over” evacuations and saving lives by preventing “under” evacuations. HVX makes it possible for web-based training allowing FEMA to train hundreds of thousands of emergency managers compared to less than 100 per year with the previous system, greatly reducing training costs and making it possible for greater numbers of emergency managers to gain critical skills in evacuation decision making.

S&T developed the First Responder Jamming Exercise. The focus of the work are the technical and operational challenges of commercially available jamming technologies on first responder communications. This work done with NPPD, FEMA, Coast Guard, Los Angeles, Houston, Arizona, NYPD among others, and brings industry to the field to work through this growing threat. S&T and OGC have 16 limited purpose Cooperative Research and Development Agreements (CRADA) in place to test equipment. From last year's exercise S&T was able to develop a training module with FLETC which was used at the inauguration to train first responders to identify and mitigate use of jamming technologies.

S&T also provided support to the response and recovery efforts from Hurricanes Irma and Harvey:

- As of Sept 12, 9 S&T surge capacity volunteers had been deployed. A system the S&T First Responders Group (FRG) and NPPD collaborated on is preparing reports on the number of businesses open and progress of business restoration. Information from the reports is being shared to emergency managers and others.
- FRG has provided approximately \$76K in communications equipment to emergency managers in Georgia to support Irma recovery. As of 11 September, the Program Manager, Shawn McDonald, the Irma ATAK server is in full deployment more than a hundred organizational users.
- S&T is providing the Android Team Awareness Kit (ATAK) technology and training to DHS components and responders Supporting Hurricanes Irma that allows them to see where and collaborate with responders and support personnel in real-time as well as to plan and track multiple locations where support/response is needed.
- S&T has used a software program to develop aerial and satellite photos that maps high-risk structures in Florida, Georgia, and South Carolina to allow for better response and recovery and made these photos available to FEMA and search and rescue teams as well.
- Flood APEX Map data sets have been completed for Georgia and South Carolina as well as Florida, in support of Irma. Flood apex has worked with ORNL to put together building outlines datasets from high-resolution satellite imagery for the GA and SC coastal counties. Previously completed initial map data sets of building structure outlines for Puerto Rico, the Virgin Islands, and south Florida and assisted FEMA with publishing those data to the web for broad community access as well as distribution to search and rescue and volunteer teams.

- S&T FRG is providing additional access to the HVX prototype system, which allows emergency managers, FEMA response officials and others to make timely and accurate evacuation related decisions more efficiently.
  - 200+ FEMA, State, and local users have been given access to HVX Prototype.
  - U.S. Army Corps of Engineers is a HVX user.
- S&T is providing a social media monitoring tool and training to allow NPPD analysts real-time updates on threats and issues including health issues, people requesting medical assistance or rescue, status of utilities and resources, and more, to allow better allocation of resources and response.
- The S&T-funded storm surge software (ADCIRC) provides emergency managers early and accurate predictions about storm surge and coastal flooding to allow them to make better decisions on evacuations, positioning of resources, and other response and recovery issues.
  - RADM Peter Brown is using the ADCIRC results to plan for evacuation of USCG staff from Key West USCG housing. On September 6, told Dr. Rick Leuttich, CRC leader, "The [ADCIRC] model was key to my decision regarding aircraft protection in Puerto Rico and our COOP decision for Miami. I'll be watching it with every update."
- The DHS S&T Coastal Resilience Center of Excellence (CRC) worked closely with the Texas State Operations Center and NOAA to provide modeling and storm surge predictions to better enable prepositioning of resources, evacuations, and recovery. The CRC ADvanced CIRCulation (ADCIRC) storm surge/coastal flooding modeling team is providing models for Texas/Gulf of Mexico. DA-E social media analysis tools: S& T's HSARPA Data Analytics Engine (DA-E) continues generating reports from open-source and social media data. The tool, requested by NPPD, monitors social media for emergent threats and augments situational awareness regarding public health and critical infrastructure. It provides automated, real-time monitoring of social media data related to public health, communications, dams, electricity, oil and natural gas and water. Urgent requests for help (e.g., infant not breathing) were forwarded to FEMA's National Watch Center. Updated reports and documents were provided approximately every 3 hours to NPPD. As of August 28, nearly 4,000 posts had been collected and analyzed to identify approximately 250 of the most relevant. DA-E also established a new collection effort on August 28 to identify an additional 100+ posts specifically focused on calls for help and will be sending these posts to FEMA. The DA-E team continues to analyze information related to infrastructure protection interests and producing regular reports. HSARPA DA-E has initiated transition of technical capabilities for situation awareness regarding critical infrastructure using open-source and social media data to NPPD.

#### SILICON VALLEY INNOVATION PROGRAM

Starting in December 2015, DHS S&T initiated the Silicon Valley Innovation Program as an effort to engage creative scientists, engineers, and technologists from across the world in solving pressing problems in National Security. As of the present time, an awareness has been built with more than 1,000 start-ups accelerators and venture capitalists. Six topic calls have been published: IoT Security, K9 Wearables, sUAS Capabilities, Enhancements to the Global Travel Assessments System (GTAS), and Enhancing CBP, Airport Passenger Processing, Financial Services Cyber Security Active Defense (FSCSAD). One hundred sixteen Phase I and 5 Phase II applications have been received. Applicants have been from across the country and international. There have been 9 Phase I awards and 4 Phase II awards to date.

#### COLLABORATIONS

For operational relevance, collaboration with users and industry is essential. The DHS S&T Cyber Security Division has developed specific and relevant collaborations with the Energy, Financial, and Automotive sectors:

- Energy sector
  - Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) is an on-going collaboration of oil and natural gas companies and DHS S&T.
- LOGIIC facilitates cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems.
- Financial sector
  - The Next Generation Cyber Infrastructure (NGCI) Apex program will identify, test, evaluate, and deploy cutting-edge technologies to deter cyber attacks against the financial sector. The program will concentrate on delivering capa-

bilities identified by the financial sector to address five primary functional gaps

- Stakeholders: U.S. Department of the Treasury, the Financial Services Sector, the OTA Contractor and private technology vendors.
- Automotive Sector
  - The (Cyber Physical Systems Security) CPSSEC program focuses include working collaboratively with automakers and leading researchers to increase vehicle cybersecurity, funding research projects to enhance auto cybersecurity, and helping to upgrade the Federal Government's fleet of automobiles.

With the successes discussed above, it is clear that DHS S&T is working towards being the agile, adaptive, and rapid innovation engine I described. That said, there is a second context to consider when evaluating the potential of S&T to be effective.

That second context is the breadth and depth of its mission and the level of appropriated funds. The S&T Budget for DoD for fiscal year 2018 is approximately \$14 billion while that of DHS S&T is approximately \$600 million. DoD has a significant National laboratory infrastructure for evolutionary capability improvements and the Defense Advanced Research Project Agency funded at approximately \$3 billion for revolutionary/disruptive improvements. In contrast S&T is asked to provide all R&D across both evolutionary and revolutionary domains with less than an order of magnitude of funding. While there is some cross-pollination possible between the departments, in many cases mission specificity and affordability factors limit the ability of DHS components to procure and sustain DoD technologies. As such, I believe that S&T is underfunded for its stated responsibilities across all of the DHS mission sets.

In fact, if the fiscal year 2018 budget cuts remain in effect there will be severe impacts to S&T ability to do its job. For example, these budget cuts will reduce the funding of the Cyber Security Division by 20% and the Chemical Biological Division by approximately 60%.

Cybersecurity is a challenge that is exponentially increasing with time. Observed malware has increased 40 times in the past 10 years. Observed attacks on critical infrastructure have increased 1.5 times in just the past 3 years. With the emergence of the internet of things, autonomous vehicles, and other networked innovations, the threat surfaces of our National security are rapidly expanding.

While awareness of the need for cybersecurity is increasing, the same is not necessarily true for chemical and biological security.

Threats from chemical and biological threat agents—known and yet unknown synthetic variations—are real, growing in potential and consequence, and becoming more attractive to terrorist organizations. As law enforcement organizations around the world make it more difficult to acquire materials to make explosives and gain access to quantities of firearms, chemical agents and eventually, biological agents will become the terror weapons of choice.

Recently, researchers at the University of Alberta announced the artificial synthesis of Horse Pox, a close “relative” of Small Pox. A number of prestigious scientific journals have refused to publish the details of this accomplishment for fear that if a step-by-step procedure were to become available, those with skills in this technology could easily produce the human Small Pox virus and unleash this terror on an unsuspecting world population.

After the attacks of 9/11, the U.S. Government recognized that defensive measures had to be implemented and maintained to protect civilians from these methods of terror attack. To this end, Congress and President Bush created a dedicated organization and facilities within the Department of Homeland Security to work closely with law enforcement and the intelligence community to identify growing threats, develop technologies to detect threats and support first responders if the unthinkable ever happened. In addition to establishing a specialized Federal and contractor workforce in chemical and biological defense technology development, two unique facilities, the National Biodefense Analysis & Countermeasures Center (NBACC) and Chemical Security Analysis Center (CSAC) were approved and funded by Congress. Each of these facilities is recognized within the United States as the Nation's focal points for biological and chemical defense awareness and response. These centers not only support many domestic Government agencies at the Federal, State, and local levels but also work closely with international partners in thwarting potential terrorists from using chemical and biological warfare agents. There is wide-spread agreement that the DHS capabilities in chemical and biological defense science and technology are unique and needed to provide a foundation for this critical area of National security. But the funding for these centers is being cut due the fiscal year 2018 budget pressures.

Given the threats to National security that our current global context mandates, I am very concerned about the impact of the fiscal year 2018 budget cuts. From my personal experience I know that one of the most disruptive forces for a technologist

and an innovation organization is uncertain and unstable funding. This challenge is magnified at DHS, because the threat environment can change on a frequent basis which can call for rapid change of investment across the R&D portfolio to meet the immediate threat. However, while I am concerned, I also believe with the appropriate support from the Department and Congress, S&T can meet the challenges of the 21st Century.

Mr. DONOVAN. Thank you, Dr. Brothers.

I now recognize myself for 5 minutes of questions.

We have a unique opportunity here. We have representatives of first responders, academia, industry, and the insight from Dr. Brothers of having served in that agency for 3 years. I would just like to ask the panel if you could share with us, if there is one thing you would like to see going forward from S&T. You certainly deal with it on a daily basis. You study it. Industry creates it. Doctor, you have seen it in use. What would you like to see this agency do? What would you like to see this committee do? What would you like to see Congress do? Aside from funding, what direction would you like to see? What is needed for our country's security from S&T that, if you had the ability, what one thing, or two things would you like to see, from each of your perspectives?

Chief.

Mr. RICE. Thank you. I would say, just from my personal experience in working on Rad/Nuc projects and planning issues around the region, I think in the chemical sector and the bio sector, a lot of the technology and data integration that we have seen with Rad/Nuc, there is a lot of discussions about it, a lot of the conferences that we go to, a lot of the meetings we attend, and I would like to see the same amount of effort that we have seen in that Rad/Nuc integration of technology apply to the chem and bio world. It seems that that reach-back capability, a common operating picture, visuals for incident commanders, it has been breaking over the last couple of years for the Rad/Nuc forum.

But when it comes to chem-bio, there is still some disconnect between the first responders and what command or emergency management might be seeing in the back. So I would like to see a greater effort in that regard, to bring those other threats up into the same level that the Rad/Nuc preparedness is.

Mr. DONOVAN. Thank you for sharing that.

Dr. Parker.

Mr. GERALD PARKER. Well, I would first, maybe, echo my colleague, that many of these, I would call it common operating picture-type things were actually called out HSPD-9 and HSPD-10 quite some time ago, so that is something else that remains elusive, and it really should not continue to remain elusive.

I think one thing, though, that I think S&T ought to be positioned so it can be a real driver of innovation. It needs to be unencumbered, and unfortunately, funding is part of that, and Dr. Brothers said it best. It is the budget uncertainty that is so disruptive. But it really needs to focus on a DARPA-esque research and innovation that can really attract the best and brightest minds across the country, whether that is in universities, whether it is in a private sector, and it has got to be nimble and agile.

I did make a comment about laboratory infrastructure in my opening remarks. Now, laboratory infrastructure, like the NBAF, NBACC, and the other laboratory, they are all necessary for the

Homeland Security Enterprise. But I think one question is, are they best placed in DHS, where there may be threats of closure, or are they best placed in their lead Federal agency for—that may have responsibility, say, for animal health, or attribution, the FBI, or DOD command authorities? Those are policy questions.

But S&T must be really agile, and innovative, and drive cutting-edge solutions that if this is impossible to do to meet near-term and longer-term needs. But we have got to be thinking about the unknown threats of the future.

Mr. DONOVAN. Thank you, Doctor.

Mr. Parker.

Mr. JAKE PARKER. I guess from our perspective, you know, in our industry, the security industry, we see a lot of innovation happening in the private sector for the commercial market, and I think that the pace of that is such that a focus on operationalizing some of these advances and innovations for Government missions would be a really high-value activity, and a focus on that.

If you look at the R&D outlook, many of those that S&T has put forward, a lot of those technology areas have seen really swift advances in the last year or 2. I think that, you know, often, you know, the Government mission requires something different, and the mission for first responders requires something slightly different, but it can be adapted for those uses, so—

Mr. DONOVAN. Thank you, sir.

Doctor.

Mr. BROTHERS. Sure. I appreciate the question. I really do appreciate the question. I think, Ranking Member, you asked a question about, you know, some of my thoughts since having been served as the under secretary. Here is one of the big things I ran into.

So S&T has to, obviously, report—I am sorry? Oh, it is not close enough? How is that? Better? Great.

What I am saying is that S&T has to report very specifically, in terms of the kinds of spends it does across the portfolio. Dr. Parker mentioned a good point; that we need kind of a DARPA-esque kind of agility.

One of the challenges, having served at DARPA and DOD, is that with the way S&T has to report early commitments and obligations of funding makes it difficult when things happen. So let me give you an example.

When I was there we had, if you probably remember, the drone landed on the White House lawn. So all of a sudden, there is concern. Now, so I have got a portfolio where all my funding has been reported where I am spending all this money. But now, I have got to respond to an emerging threat. How do I do that?

So the agility that Dr. Parker is talking about, and I applaud, I don't have the tools to make that happen, because I can't move money like that, even though there is an observed threat.

So I think one of the things that we need help with is how do we understand your role as a short oversight, and the effective and efficient use of funding? How do we also give S&T the ability to be agile with this funding, when we have these emerging threats that we didn't necessarily predict, you know, the so-called black swan events happen? How do we handle that? It is an issue.

I think more specifically, we have done a good job. S&T has done a good job of reaching out to industry through the Silicon Valley Program, for example. One of the tools for doing that, the investment vehicles, calls it other transactions authority, other transactions.

This has come up a number of times. I think S&T does need the authority for that, as opposed to going through management, so I think that is something that S&T could definitely use as well.

Something that is more inside the Department, but could be encouraged, is better integration into the acquisition process itself. Because I think you are probably familiar that with all S&T organizations, whether you are talking about DARPA, or the DOD laboratories, or S&T itself, fundamental challenge is what? It is the valley of death, as people call it, right? That valley of death is when you have to come up with a research prototype. A prototype has a lot of the capabilities you need, but it is not manufacturable at that point.

How do you get that prototype, that concept in the actual acquisition process? That is a challenge all research organizations has. But I think it would be an encouragement to actually better integrate that into the Department's way of thinking, the Joint Requirements Council, for example, which is part of the way the Department is moving toward some of the more process-oriented ways of doing requirements that the Department of Defense has. How do you integrate these systems better?

You mentioned the IPT process, and the IPT process, I think, is an important process, and it is, for the first time, really tried to give S&T an opportunity to focus on agreed-upon Department capability priorities. There are challenges there though, right? The challenges there are that that is a year-long process. So that means that you do not really start working on those until the next year. So again, you have a delay.

So how do we get more speed in this innovative process? That is a start, but we need to be able to handle these type, like I said, these emerging technologies, emerging threats in a much more rapid basis.

So I think those are some of the areas I would encourage you to look at.

Mr. DONOVAN. Well, I thank you all for your insight.

My time is expired. The Chair now recognizes the gentleman from New Jersey, the Ranking Member, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Dr. Brothers, as you know, the Science and Technology Directorate is still operating without a permanent under secretary. How important is it that S&T have a strong leadership and clear direction in place, as it carries out its mission?

Mr. BROTHERS. Sure, thanks for the question. I think it is very important, and the reason why I say that is even though there is fully capable leadership from career, as well as acting under secretary currently, typically, what you find happens is that changes don't happen, because everyone is waiting for the political appointee to actually come on board.

Until that happens, you know, not a lot changes, and I think one of the challenges we have, as I think many of the panelists here

have agreed: We have a very fluid threat environment, and we have to be ready to adapt to this. Without strong leadership on top, that is not really possible right now. So even though I think we have made good changes, I think we need leadership that is going to be able to keep up with the change that we are seeing in our threat environment.

Mr. PAYNE. Let us see. Mr. Parker, would you like to weigh in on that?

Mr. JAKE PARKER. Absolutely. I think that is, I would definitely agree with Dr. Brothers that, you know, there has definitely been, you know, the folks we have worked with, the S&T, I think, many of them are new in their positions in the last couple months. They have some great ideas about what they want to do, but they need, you know, leadership from the top to give them their green light to proceed, and so that is, I think, what Dr. Brothers was getting at.

Mr. PAYNE. Dr. Parker.

Mr. GERALD PARKER. I totally agree. There is outstanding professionals there in the Department that are keeping things moving. But the—it is, again, it is the uncertainty. Who it is going to be, when are they going to come in? They are ready to roll up their sleeves and work very hard, but it is the uncertainty that is, it is really, I think, an issue.

Mr. PAYNE. Possibly going in a totally different direction than they have been?

Mr. GERALD PARKER. Well, you know, I don't know that, but I think it is really more the uncertainty. I think Dr. Brothers did a whole lot to steady the ship, so to speak, in S&T. The command culture has greatly improved, and people are happy to come to work, and they are working hard, and you don't want to lose that momentum. We have threats that we face every day, and we can't wait 'til—we can't wait.

Mr. PAYNE. Chief Rice.

Mr. RICE. Thank you. Yes, I would have to agree with my colleagues here, that that leadership needs to be there, and it needs to be strong. On a personal level, and in our interactions with the folks down at NUSTL, it came as quite a shock that, you know, they may have been on the cut side of this. But, you know, they rolled up their sleeves, and they continue to work on their portfolios, and continue to contribute and make positive impacts for us on the responder side. So having that leadership in place so that they can reaffirm their mission and continue this work going forward is critical.

Mr. PAYNE. OK. Dr. Brothers, when you first were named under secretary of science technology, you told me that one of your priorities was to energize the homeland security industrial base. What are some of the challenges that you experienced trying to attract businesses to participate in the homeland security industrial base?

Mr. BROTHERS. You know, one of the biggest challenges—and Mr. Parker brought this up—with the new outreach to industry that you were mentioning. It is communication, right? I think one of the biggest challenges is that industry would, of course, like to solve these challenges. They don't necessarily know what those challenges are. They don't necessarily know who to talk to in a depart-

ment, who to email. They don't necessarily know what the funding looks like.

I think that is still an issue. It is not just unique to DHS/S&T. But I think one of the biggest challenges I have had was actually communicating what are our needs, who do you talk to, and what kind of funding is out there.

Mr. PAYNE. OK. Let us see. As you know, the President's fiscal year 2018 budget submission was criticized for its massive cuts to the Science and Technology Directorate budget. What message did the budget send to the stakeholder community about the administration's commitment to research and development at S&T?

Mr. BROTHERS. Well, I mean, the way I take that is that it is much lower priority, and I think as I mentioned in my opening statement, my concern is when we are in an environment where the threats are increasing, that, I think, is the wrong message. I think we need to be messaging that we see this research and development working with industry as essential for our defense. I don't think that is the message that the budget shows.

Mr. PAYNE. Mr. Parker.

Mr. JAKE PARKER. Yes, I would agree. I mean, the message would be uncertainty about the future, and that is the, you know, very concerning. Obviously, there are other things in that submission, too, really, the DHS, particularly FEMA grants that we would be very concerned with as well. But uncertainty would be the message that I would send.

Mr. PAYNE. Dr. Parker.

Mr. GERALD PARKER. Yes, there is no doubt that the threats that we face are actually going to require a strong innovative science and technology approach. No doubt, our emergency operations and so forth are part of it as well, but we have a lot of unknown threats, and it will require the scientific engine of this country to address these threats. So the budget cuts to research and development, S&T does not send a good signal to the community that I come from.

Mr. PAYNE. OK.

Chief Rice.

Mr. RICE. I agree with everything my colleagues said. I have no further comment at this time.

Mr. PAYNE. Well, I see that my time has expired, so I will yield back.

Mr. DONOVAN. The gentleman yields. The Chair recognizes the gentlewoman from New Jersey, Ms. Watson Coleman.

Ms. WATSON COLEMAN. Thank you, Mr. Chairman, and thank you all for being here today.

I want to follow up, I guess, on both what the Chairman and the Ranking Member were talking about, but perhaps from a different perspective. As—and this has to do with the Trump administration's fiscal year 2018 budget cuts. I know some of those cuts have been restored through an appropriations process, but we still are grappling with some serious underfunding.

You all have been asked by the Chairman on the first sense what is it that you think—what is it you would like for us to do? What is it you think that the agency should do? What would be the priorities?

I would like to know, from your perspective, based upon some the things that you said—agility, innovation, identifying the brightest and the best, working with private sector, et cetera. Tell me, from your perspectives, each of you, if you don't mind, what this budget does specifically to accomplishing those things that you said were vitally important, from an operations perspective.

I will start with you, Chief.

Mr. RICE. Specifically, what the S&T Directorate does for us, from an operations perspective, or was it a budgetary question?

Ms. WATSON COLEMAN. What is, yes. How does this budget impact those things that you are interested in in this directorate? Responding to the Chairman having said what would you think we need to do, and then you indicated some issues with regard to agility, and innovation, and, you know, to be able to move and respond to different threats.

So I want to know, with the cuts that are proposed, so this budget that is proposed, what specifically impact would it have on where you think this directorate should be going?

Mr. RICE. Yes, thank you, Congresswoman. So I think, as my colleague mentioned, you know, the emerging technology is going at such a rapid pace, as is the evolving threats, and that cuts to this program, and cuts to S&T will hamper our ability to keep up with those technologies and those threats, and as our equipment comes to reach its life expectancy, and as further threats evolve, we will start to lose pace with those, and not be on the cutting edge of preparedness and response.

Ms. WATSON COLEMAN. Thank you.

Dr. Parker.

Mr. GERALD PARKER. Yes, I may mention something that hasn't been mentioned yet in regards to the cuts. There is also a proposed cut to the university Centers of Excellence effort. So what will that mean? I don't know, but as possibilities are decreased numbers of Centers of Excellence, decreased funding to that. So there is decreased university input as being part of the solution for homeland security.

I think it has another effect, and that is affecting the next generation. I know one of things that we do at Texas A&M is really focus on, and we have been able to leverage having a Center of Excellence to make sure that we give opportunities to students and student interns, graduate students. So they get exposed to homeland security issues, and maybe take a career in homeland security. So I think this is also going to have an effect on the next generation, and diminish the number of people who take a career path in this area.

As I said in my opening statement, and thankfully, some of the budget has been restored to save closure of the NBACC. But I can't imagine if that were closed, what our ability to be able to bring to bear microbial forensics and attribution for potential biological attack, or trying to differentiate a natural from a biological attack. That could be catastrophic.

Ms. WATSON COLEMAN. Thank you.

Mr. Parker.

Mr. JAKE PARKER. So I know, you know, much of what was proposed in the budget has been restored through the appropriations

process, as my colleagues mentioned. But, you know, as proposed, as Dr. Brothers mentioned, the budget would have cut chem/bio by 60 percent, cybersecurity by 40 percent. I think that, I guess, the impact of that could be that you would slow the development of some really important technologies.

I was just talking recently with one of our member companies, who was working on a project funded through the chem/bio portion, about—that would basically now enable smart buildings to detect chem and bio threats on an affordable basis. Something that our industry is working on, you know, generally, is building security. That would be, you know, a great addition there that could, especially in urban areas, that could be important also.

On the cybersecurity front, there is a company that is involved in application security in mobile devices at a very high level. It is something that they could possibly be affected by, so—

Ms. WATSON COLEMAN. Thank you.

Dr. Brothers.

Mr. BROTHERS. So I think I can be general, and then get to some specifics. Mr. Parker just mentioned specific budget cuts to both cyber—well, to cyber and the bio division.

So the bio division, they are interested in expanding the work they are doing in New York City to not just look in the subways, but also to look at a test-bed for bio security. The challenge is, how do you do this when your budget is being severely cut? How do you do that, starting kind-of a new initiative? How do you do that? It is a challenge.

The cybersecurity division: I mentioned how they are reaching out to industry—financial, automotive sectors, energy sectors. Again, this all takes funding. They are doing this to increase the cybersecurity of our critical infrastructure. They are also reaching out to industry, this in Silicon Valley, Austin's, Boston's, District of Columbia's, et cetera, to reach out to the creative communities around the world. Again, need the funding for that.

I think there are a number of challenges with—actually, I want to go back to what Dr. Parker said about the Centers of Excellence. Let me give you an example, if I can.

I was at USC, and actually, before that, I was at LAPD. They have instituted something called predictive policing. In predictive policing, they were using technology to actually reduce crime by 14 percent in certain areas.

I then went to USC, which was one of DHS's Centers of Excellence. What they showed was that using game theoretic techniques, they were able to improve that to almost 25 percent.

So the importance of university research shouldn't be understated at all. It is part of the S&T ecosystem—the laboratories, universities, Government, industry, et cetera. So I think these budget cuts impact that entire ecosystem. But in specific ways, you can look at programs that DHS has, S&T has instituted, and they get impacted directly.

Ms. WATSON COLEMAN. Thank you. Thank you. I see my time is up.

Thank you, Mr. Chairman. I yield back.

Mr. DONOVAN. The gentlewoman yields back. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for your testimony this morning.

I thank my colleague, Ms. Watson Coleman, for addressing a lot of the things that I have in my questions, so I am going to give you an opportunity to elaborate on some of those topics, both chem/bio in particular, and cyber.

Dr. Parker, I would like to just start with you, if I could. As you mentioned in your testimony, the President's budget request for fiscal year 2018 ends DHS's S&T funding for the state-of-the-art, one-of-a-kind biocontainment laboratory, the National Biological Analysis and Countermeasures Center, the NBACC facility at Fort Detrick, Maryland, and without transferring the responsibility for operating the facility to different a department or agency. So can you elaborate on the impacts on National security and law enforcement if this facility were to close?

Mr. GERALD PARKER. Yes, thank you for the question. The NBACC, and then specifically—actually, both missions of the NBACC, the threat assessment and the forensics, bioforensics mission was—actually, I had something to do with the original vision, back when I was at the United States Army Medical Research and Material Command, and then subsequently, in DHS's S&T. It was a strong collaboration between the FBI, law enforcement, the intelligence community, Defense, and then it was the Office of Homeland Security, before it became the Department of Homeland Security.

So this laboratory facility has had a lot of thought that went into why it was needed, what capabilities it required to support what was a new science that was born out of the anthrax letter attacks, and that was microbial forensics. So it really is a very key mission in trying to determine who may be responsible for a biological attack, whether it is an individual, whether it is a terrorist, whether it is a nation-state. Those are no-regret decisions, as well. So the science and everything associated with what is needed for a law enforcement investigation has got to be beyond reproach.

So there was a lot of thought that went into this, and I certainly would not want to be in the National Command Authority, and we had to make decisions about retaliation, say, for a nation-state bio-attack—that is not out of the realm of possibility today—unless I knew that science behind the microbial forensics was solid. It is a no-regret decision. That is the impact that we have with that laboratory potentially closing.

Mr. LANGEVIN. Thank you. I appreciate the answer, and I agree. I hope that that is going to be something that will be reversed as we go through the budget process, and get through the appropriations process. That is something that I hope is going to reverse itself, so, and so it is something that I will advocate for.

Dr. Brothers, if I could thank you for being here. It is good to see you again before the panel. I always appreciate your candor, and your testimony. I just want to thank you for all your work securing the homeland, and all the things you have done to improve DHS.

So DHS specifically, the Science and Technology Directorate has funded important cybersecurity research to protect the homeland. I know you had this conversation just a minute ago. For instance,

though, S&T grants have played an important role in catalyzing research to catalog free and open-source projects that represent the core internet structure, infrastructure. Obviously, it is vital to understand which libraries are integral to critical infrastructure in order to ensure that they are adequately secured, and which is why the S&T support really has been so important.

So needless to say, this research is just one example of many that the directorate supports in this emerging security domain. You know, just to further elaborate on the cybersecurity front, based on your experience, how would cutting-edge—how would cutting the cybersecurity research budget, as proposed by the Trump administration, affect the ability of DHS to secure the homeland?

Mr. BROTHERS. So I think one of the challenges that we run into—and the panel, we have said this a couple times—is emerging threats coming out. One of the things that DHS/S&T, the Cyber Security Division as well, is try to think ahead, right? Think ahead.

So here is an example, autonomous vehicles that I mentioned a little bit earlier. A number of years ago, the Cyber Security Division started working with industry to think about, what are going to be some of the challenges securing not just autonomous vehicles, but networked vehicles? So there are a lot of conversations about smart transportation, right? This is where you have got cars that are communicating with infrastructure to improve the transportation experience, if you will, right?

The challenge is, what if you hacked into that? One of the things that Cyber Security Division did was to start thinking about that early on, and develop a consortium of automotive makers to try to address some of those issues.

The same is true getting the oil and gas companies together in a program called LOGIIC to think through, what are some of the threats to the infrastructure?

So the challenges you run into is that when you look at infrastructure that is privately owned, there is not necessary the motivation to start thinking ahead for these kinds of things. But the motivation is there for the Cyber Security Division and the rest of S&T.

So in thinking about 20 percent budget cuts to the Cyber Security Division, those are the kinds of things that get impacted, is that ability to look ahead, the ability to invest moneys to understand what potential problems there will be with emerging technologies and develop mitigating solutions.

Mr. LANGEVIN. Thank you.

Mr. Chairman, I have one brief last question. Would that be all right?

So Dr. Brothers, one last question. So cybersecurity, obviously, is an international issue by its nature. How essential to securing our Federal networks and critical infrastructure is cooperative research and development with our international allies? What are some of the examples of successful projects that S&T has supported in that?

Mr. BROTHERS. Yes, that is a great question. I think one of the things that we have to realize is that because of the hyperconnected nature that we live in, technology, this kind of engineering side of expertise is really democratized. Everyone has

this. So we don't necessarily have the only best ideas. It is important that we reach out to all the people—our friends, our allies—to try to understand what some of the best ideas are out there.

We have relationships. We have 13 bilateral relationships across the world, and we leverage all of those, in cyber as well as in some of the other areas as well to try to get some of the best advantages. We have actually started the idea of having, with the Netherlands, with having a mutual—with joint BAs, broad area announcements, meaning that we now work with the Netherlands to put out solicitations to the international community.

So it is that kind of joint work that DHS is doing—DHS/S&T is doing to leverage the entire global ecosystem of creative thinkers.

Mr. LANGEVIN. Dr. Brothers, thank you very much.

Thank you all, the witnesses, for your testimony, and Mr. Chairman, thank you for the latitude in being able to ask that last question.

Mr. DONOVAN. Absolutely.

We have such an advantage of having the four of you here. I just asked the ranking Chairman; I think we are going to just let each Member have 2 more minutes with you, just because we have you here. My one question to all you, because your testimony was incredible. Your efforts to protect our Nation, we are so grateful for.

As you are doing this research, Doctor, as you were speaking about reaching out to others, how do we protect what we discover? Everything we create, the bad guys try to intrude on. So without divulging trade secrets or National security issues—and I promised my colleagues, we are only going to get 2 minutes each, because we have to let you go. I know the chief has to get to another part of our Nation right now.

The challenge I see, besides creating these great things you are speaking of, is how do we keep them to us? If you just have a thought about that, and then I am going to pass the questions on to my colleagues.

Mr. GERALD PARKER. Yes, I will just, I will start. You know, it is an excellent question. I am not sure if I have the best answer, but it is a must that we protect our science, and secure our science.

I would actually maybe recommend that you talk to a very good colleague and friend of mine from the FBI, Special Agent Ed Woo, who has thought about this topic a lot. He used to think about it just in the terms of biosecurity, but it is really emerged into how do we—it is protecting our science. How do we do it securely? Perhaps, maybe universities have the biggest challenge, but it is an area that I know that Texas A&M takes very, very seriously, and—

Mr. DONOVAN. I suspect you have to report on your research if you are using Federal monies for it—

Mr. GERALD PARKER. Of course.

Mr. DONOVAN [continuing]. And do you protect your—

Mr. GERALD PARKER. Yes, of course. Of course.

Mr. DONOVAN [continuing]. Your research. Doctor, how do we protect this stuff?

Mr. BROTHERS. It is hard. It is hard, and we all know about the cyber intrusions, that kind of thing. I think there are a number of people, including S&T, looking at different architectures for cyber

defense. There are people looking at different ways of encrypting information, whether that information is in storage, transit, or in computation. That can help.

But I think you also have to consider there are different paradigms, because of democratization of all this knowledge. You can't keep everything secret. So the question is: How do you continue to innovate even more rapidly? Because part of it is going to be not just keeping things secret, but it is going to be outpacing the innovation of our adversaries, and never stopping, and that is what requires the agility and adaptability we were talking about earlier.

Mr. DONOVAN. Thank you, Doctor.

I already violated my 2-minute rule. The Chair recognizes the Ranking Member from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Dr. Brothers, during your term as under secretary of science and technology, you took a number of steps like reinstituting the integrated product teams to create formal channels of R&D coordination among DHS components. Can you elaborate on some of the obstacles the directorate faces when it comes to streamlining and coordinating R&D throughout the Department?

Mr. BROTHERS. Sure. One of challenges just is a large organization, large bureaucracy, right? So you have a lot of different stakeholders. So the IPT, again, the Secretary signs that out. That is excellent, because that gives some top-level mandate to that.

But then you have other processes. You have got the Joint Requirements Council is a process. It has to be approved through the DMAG, these kinds of things.

So a lot of it is messaging and socialization, and I think those—it is all in culture, right? I mean, a lot of these big organizations, they struggle because of culture. You look at an organization like DHS has multiple cultures because of the way it was created. How do you create a joint culture that understands what S&T is doing in the larger context, as well as the context that each individual component has? I think that is one of the biggest problems. It is not so much the IPT process, or convincing people it is a good idea. It is how do they accept it, and how do you message to them how this is a good thing for them as well? It is a work in progress.

Mr. PAYNE. Thank you.

Mr. Chairman, I have more of a statement than another question. I think, as we have gone through this process, we see how important S&T is with the evolving threats that we have in this area, and with the world. I think it is incumbent upon us to continue to have the administration, whichever administration it is, understand how important this is, because when we are attacked, and God forbid, when we are, we are always sorry and remorseful after it. But if we can do the things that we need to do to thwart it, then we wouldn't find ourselves in that position.

We have to get the administration, regardless of whatever administration it is, to take this seriously, and put in place a budget that is consistent, and would allow S&T to do the work and the type of things that it needs to do to make sure that we are successful in this area, and I yield back.

Mr. DONOVAN. The gentleman yields, and I hope that your testimony didn't scare my colleagues, who left to go protect themselves somewhere in a bunker.

I want to thank our witnesses, first of all, for your valuable testimony; second, for your contributions to the safety of our Nation. I would like to also to thank my colleagues for their questions.

The Members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond to those in writing. Pursuant to committee Rule VII(D), the hearing record will be held open for 10 days. Without objection, the subcommittee stands adjourned.

Thank you all.

[Whereupon, at 11:16 a.m., the subcommittee was adjourned.]

