

Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)
Homeland Security Science and Technology Advisory Committee (HSSTAC)

April 7-8, 2014

1120 Vermont Ave. NW

Washington D.C. 20005

MEETING MINUTES

SUMMARY: This was a two-day meeting, and the second to focus primarily on S&T's relationship with DHS components. The December 2013 meeting focused on Customs and Border Protection (CBP). This meeting focused on Immigration and Customs Enforcement (ICE). Day 1 of this meeting was devoted exclusively to ICE and included briefings from ICE and S&T officials and feedback from HSSTAC members. Day 2 featured three informational S&T briefs and a closed session to discuss classified and industry-sensitive information. Attendees included all nine current members of HSSTAC, 10 members of ICE, about 50 other members of DHS, and three members of the public. (See attendee list at end.) Meeting materials, including the slides mentioned below, are posted at <http://www.dhs.gov/st-hsstac>.

April 7, 2014

1. CONVENE

DHS Under Secretary (Acting) for Science and Technology Daniel Gerstein convened the meeting at 9 a.m.

2. INTRODUCTIONS AND AGENDA REVIEW

Gerstein summarized the agenda and made introductions.

3. ICE OVERVIEW

(For related slides, go to <http://www.dhs.gov/st-hsstac>. Scroll to “Past Meetings,” then “April 7-8, 2014.” Select “Meeting Briefs.” Then select “HSSTAC ICE Presentation, April 7.”)

Immigration and Customs Enforcement (ICE) Deputy Director Daniel Ragsdale gave an overview of the ICE organization, beginning with an explanation of three directorates: Homeland Security Investigations (HSI), Enforcement and Removal Operations (ERO) and Management and Administration (M&A). He described a “Day in the Life” of HSI and ERO and the organization of M&A. He emphasized the need to need to increase efficiency, automate, and put technology into the hands of operators. He described ICE’s focus areas for R&D and innovation in 2013/2014. He described the Cybercrimes Center (C3) and the emphasis on cyber forensics. He described the entity called Technical Operations (TechOps) and how it works with S&T, including the recently-completed low-light camera and Encrypted Video Encoder System. He emphasized the importance of tunnel detection and child exploitation. Regarding HSI, he emphasized its operational bent, and the fact that it focuses on both physical and cyber borders.

A discussion followed with committee members concerning jurisdictions; the role of intelligence; the Nogales tunnel in Arizona (and how the DHS Science and Technology Directorate (DHS S&T) is working on the technical aspects); international cooperation (Immigration and Customs Enforcement (ICE) has the largest international footprint within DHS); public-private partnerships (which could be more robust); and links with other agencies (for example, the U.S. Secret Service). Ragsdale commented on the importance of working with S&T to ensure that ICE requirements are sound.

4. **ICE Homeland Security Investigations (HSI): Cyberforensics, Technical Operations, Surveillance, and Tracking**

Eric Feldman, Unit Chief, Cyber Crimes Investigations, commented that ICE’s Cybercrimes Center (C3) relies heavily on S&T, especially regarding the technical aspects of cybercrime. He described C3’s origins within Immigration and Naturalization Service (INS) and its general strategy to “follow the money.” He identified HSI’s three units: child exploitation, cybercrimes, and computer forensics. He emphasized its Emerging Technologies Program, which began 18 months ago. He identified key Research and Development (R&D) gaps: the Silk Road (and the free software called Tor, which enables online anonymity); cyber training; and image analysis related to child exploitation, which is enabled by Tor. He emphasized the international nature of cybercrime and ICE’s relationships with foreign partners. He mentioned the move from prosecutorial focus to victim focus. He described ongoing work with DHS S&T, primarily the Cyber Security Division (CSD) and the Small Business Innovative Research (SBIR) program. He identified as a capability gap the ability to ingest large amounts of data. He also mentioned digital theft of intellectual property (a center in DC focuses on this) and digital theft of export of data (a more recent effort).

A discussion followed with committee members regarding responsibilities to prevent or respond to cybercrimes; the rapid development of malware; the role of social media in cybercrimes and its constant evolution; and C3’s frequent interaction with S&T’s CSD.

Kelly Oliver, Section Chief, Technical Operations (ICE HSI Tech Ops) described the role of Tech Ops to provide the latest technology to investigators in field. He discussed the role of the Technical Enforcement Officers (TEOs) as “investigative force multipliers” and the success of the cross-agency Covert Video Working Group (CVWG), which involves 20 federal agencies and is facilitated by HSI Tech Ops. He presented a video demo of the low light camera (which was vendor-led vs. requirements-led) and the Internet Protocol (IP) encoder. He identified future emphases for S&T collaboration: integrate sensors, decrease band-width, miniaturize systems, and energy consumption. He added that a tie to biometrics is still on the wish list.

5. ICE - Tools and Safety

Bert Medina, Assistant Director, Office of Firearms and Tactical Programs (OFTP), described OFTP’s mission to serve 62,000 armed officers at DHS and to ensure that ICE can conduct its law enforcement responsibilities. He emphasized that as budgets get tighter, it’s more important than ever to leverage technology. One advantage of OFTP, he said, is its robust laboratory which does testing. He described the virtual shooter program, developed as a Small Business Innovative Research (SBIR) program in cooperation with S&T’s First Responder Group (FRG) and now going to SBIR Phase II, with delivery planned in spring 2015. The focus is officer safety; the goal is to quantify design characteristics in handguns that make it easier to shoot, and ultimate commercialization. Immigration and Customs Enforcement (ICE) wants to drive the design but wants the commercial sector to develop it.

A discussion followed with committee members regarding whether this is a defensible focus in a time of diminished resources (Immigration and Customs Enforcement (ICE) feels it is, because it saves time and money, improves officer safety, and is requirements-driven), and whether the technology has been shared (it has been shared with Department of Defense (DoD), which is working on a similar project). In response to a question about what keeps him up at night, Ragsdale responded that he is concerned about resources, the various forms of fraud, and detention/immigration (i.e., the need to be humane and detain as briefly as possible).

6. S&T OVERVIEW

(For related slides, go to <http://www.dhs.gov/st-hsstac>. Scroll to “Past Meetings,” then “April 7-8, 2014.” Select “Meeting Briefs.” Then select “HSSTAC Day 1 Brief - April 7, 2014.”)

Gerstein explained the four groups that comprise DHS S&T. He pointed out that two technical divisions work closely with ICE: the Cyber Security Division (CSD) and the Borders and Maritime Division (BMD). He added that DHS S&T also works with ICE on Big Data. He described the value-added proposition which aims to align S&T more closely with operators. He emphasized the importance of innovation and the importance of assessing technical risk. He also emphasized the importance of partnerships to save money (for example, with DoD). He then asked the four group leads to summarize their responsibilities.

Adam Cox, Acting Director, Homeland Security Advanced Research Projects Agency (HSARPA), DHS S&T explained the five divisions that comprise HSARPA. (Slide #8)

Greg Price, Program Manager, Responder Solutions, First Responders Group (FRG), explained FRG's mission and focus areas, emphasizing that FRG partners with first responders representing 70,000 agencies nationwide, and it issues an annual report on first responder needs. (Slide #9) **Jim Tuttle, Chief Systems Engineer, Office of Systems Engineering, Acquisition Support and Operations Analysis Group (ASOA)**, described ASOA's six capabilities. (Slide # 10) **Keith Holtermann, Director, Research and Development Partnerships Group (RDP)**, explained that RDP supports the other internal groups and also does external outreach to extend the reach of S&T. (Slides # 11, 12.) A brief discussion followed with committee members about DHS' approach to systems engineering and the appropriate balance between research and development. Gerstein commented that 21 roadmaps should be in final form by June 2014.

7. HOW S&T SUPPORTS ICE: BORDER ENFORCEMENT ANALYTICS PROGRAM

(For related slides, go to <http://www.dhs.gov/st-hsstac>, "Past Meetings," "April 7-8, 2014." Select "Meeting Briefs," then "HSSTAC Day 1 Brief - April 7." Go to slides #13-15.)

Steve Dennis (Apex Program Manager, Homeland Security Advanced Research Projects Agency, DHS S&T) and **Thariq Kara (Program Manager, Office of Chief Information Officer, Immigration and Customs Enforcement)** described the Border Enforcement Analytics Program (BEAP), which is one year old, and its three primary deliverables: a "big data" test enclave, operational testing, and deployment of big data tools to the customer. They emphasized that Big Data is a wide-open field, and transition to operational can be very difficult. They identified geo-coding and language translation as two important needs.

A discussion with committee members followed concerning analytics, storage systems, and the implications of this program for other DHS entities.

8. HOW S&T SUPPORTS ICE: CYBERFORENSICS

(For related slides, go to <http://www.dhs.gov/st-hsstac>, "Past Meetings," "April 7-8, 2014." Select "Meeting Briefs," then "HSSTAC Day 1 Brief - April 7." Go to slides # 16-27.)

Megan Mahle (DHS S&T Cyber Security Division) described the Cyber Security Forensics Project, which began in 2009 to fund specific law enforcement requirements. She described the Cyber Forensics Working Group (CFWG), comprised of about 100 members -- including ICE Homeland Security Investigations (HSI) Cybercrimes Center (C3) -- which identifies needs based on actual casework. She emphasized that S&T is trying to do extensive testing with law enforcement; however, law enforcement is a small piece of the market for technology developers. She gave some examples of funded requirements and described a forensics project called Blackhorn3, a tool to analyze evidence from handheld and maritime Global Positioning System devices which is now available commercially. As other examples of S&T projects that involve or may impact ICE, she described a triage field kit for first responders; a vulnerability assessment of the Wireshark high-speed data capture tool; disposable cell phone forensics; flash memory chip analysis, which is an Small Business Innovative Research (SBIR) project; open source acquisition and analysis tools;

solid state storage forensics, also an SBIR project; the National Institute of Standards and Technology Computer Forensic Tool Testing project and the National Software Reference Library; a cyberforensics electronic technology clearinghouse called CyberFETCH, which is broadly accessible; and a global cyber security law enforcement technical symposium called GCSLETS, which is by invitation only.

A discussion with HSSTAC members followed concerning standards, testing, access, the challenge of remaining current, and the value of the open-source community (CyberFETCH).

9. HOW S&T SUPPORTS ICE: BORDERS AND MARITIME SECURITY

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides # 29-36.)

Jon McEntee, Acting Deputy Director, Borders and Maritime Security Division (BMD), Homeland Security Advanced Research Projects Agency (HSARPA), DHS S&T gave an overview of BMD mission and portfolio and listed projects in three areas; land borders, maritime borders and cargo. He explained that among DHS components, BMD primarily supports the United States Coast Guard (USCG), Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE). He mentioned efforts that currently support or may interest ICE: robotic aircraft for public safety (with a focus on first responders); small dark aircraft detection (to detect, track and classify low-observable aircraft entering the U.S.); tunnel age determination (through soil analysis and testing); clandestine tunnel detection (using modeling and simulation tools); in-the-mouth tactical communications (transmits sounds through bone conduction); coastal surveillance system (fusing nodes to provide more situational awareness); underwater remote operated vehicle, or BIOswimmer (for underwater surveillance and vessel inspection); counterfeit goods detection (using vapor signatures); bulk currency detection (seeking better screening capabilities); hand-held backscatter X-ray scanner (for vessels and conveyances); and general aviation aircraft scanner (a mobile unit to quickly scan the inner voids of an aircraft).

Discussion with committee members focused on the detection of small dark aircraft (whether the threat is increasing and if so, how this project may help address the threat given declining resources); the diversity and challenges of land border security, including geography; and the large number of containers (32,000) that arrive in U.S. ports every day. Further discussion followed about how to determine priorities during steady-state or declining resources, and the need for trade-off analysis.

10. HOW S&T SUPPORTS ICE: LOW-LIGHT CAMERA

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides # 37-40.)

Greg Price, Program Manager, Responder Solutions, First Responders Group (FRG), DHS S&T, re-reviewed the Low Light Camera and Internet Protocol (IP) Encoder Project mentioned in the morning session, which responded to a requirement from ICE Homeland Security Investigations (HSI). The encoder will be available June 2014; further work is being

discussed. Kelly Oliver (ICE) interjected that ICE had a clear vision of what they wanted, and called it a successful collaboration.

11. HOW S&T SUPPORTS ICE: CBP-ICE ALIEN PROCESSING SYSTEMS ANALYSIS

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides #41-42)

John Dargan, Director, Research and Development Analysis and Assessment Office, Acquisition Support and Operations Analysis Group (ASOA), DHS S&T, discussed a project, worked jointly with CBP and ICE, to make the alien process flow more efficient and effective. He also discussed the Port Isabel Detention Center Systems Analysis Project, which will enable ICE to make analytically-informed decisions regarding operations and acquisitions. He discussed the project sequence: define the problem, establish vision and success criteria, describe the current process, and determine requirements. He pointed out that CBP undertook two reforms identified by this project, resulting in financial and time savings (about 2,000 hours per month) for CBP. The project is focusing now on seamless custody transfer between CBP and ICE. ICE is assessing about 30 recommendations received under this project to determine which will be most beneficial.

12. HOW S&T SUPPORTS ICE: CENTERS OF EXCELLENCE

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides #43-48.)

Matt Clark, Director, Office of University Programs (OUP), Research and Development Partnerships (RDP), DHS S&T gave a summary of OUP’s programs, nine centers of excellence (COEs), and current projects with ICE. He emphasized the National Center for Border Security and Immigration (NCBSI) as the COE most directly serving ICE. He also emphasized the Center for Visualization and Data Analytics (CVADA) and its project for automatic recognition and interpretation of gang graffiti (GARI), which analyzes graffiti from mobile devices. He described two joint efforts supporting ICE: one addresses unaccompanied alien children and involves three COEs; the other seeks to analyze transnational criminals’ use of social media in the El Paso Region and involving two COEs. He encouraged more ICE involvement in the COEs and suggested three possible areas: resource optimization (following a successful model with USCG); economic impact analysis (following a study for CBP regarding the impact of staffing on wait times); and data and visualization (using a visual analytics tool developed by CVADA).

Discussion followed with committee members regarding how COEs are evaluated, the use of peer review, funding of COEs, component engagement, and measures of success. Clark pointed out that one measure of COE value is how much money they receive; currently \$28-30 million per year from S&T and at least \$75 million from other sources. He emphasized the need for a clear end state; after two years, a COE must transfer results to an end user or face cancellation.

13. HOW S&T SUPPORTS ICE: ENGAGEMENT WITH DOE LABS

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides # 49-52.)

Jamie Johnson, Director, Office of National Labs (ONL), RDP, DHS S&T gave an overview of the five internal Science and Technology (S&T) labs and the 17 Department of Energy (DOE) labs, of which 13 conduct homeland security (HS)-related research. He commented that ICE would benefit most from the Department of Energy (DOE) labs which do HS research, focus on long-range technology development, and also provide “rapid response” during national emergencies. He reviewed the agreements and authorities of the DOE national labs and how to access their services. He then summarized the capabilities of the DOE national labs, citing cyber analytics and big data in particular. He then reviewed two projects of interest to ICE: Trade Enforcement Technology Solutions (to identify, develop and integrate an advanced suite of cyber analytics tools which enhance the ability to disrupt smuggling networks) and a Tagging Tracking and Locating (TTL) Feasibility Study (involving cell phone applications, state-of-the-art identification technology, and tools to identify smuggling networks). He emphasized that it’s not hard to do business with the labs, but Department of Energy (DOE) has not done much with Immigration and Customs Enforcement (ICE) so far.

14. HOW S&T SUPPORTS ICE: OPERATIONAL EXPERIMENTATION PROGRAM

(For related slides, go to <http://www.dhs.gov/st-hsstac>, “Past Meetings,” “April 7-8, 2014.” Select “Meeting Briefs,” then “HSSTAC Day 1 Brief - April 7.” Go to slides # 53- 54.)

Charles Edwards, Director, Interagency Office, Research and Development Partnerships (RDP), DHS S&T provided an overview of the Operational Experimentation (OpEx) Program. He described ICE involvement in Joint Interagency Field Exploration (JIFX) events, in which ICE identified 10 potential technologies. He discussed current collaboration with ICE involving tunnel mapping and robots, and highlighted upcoming OpEx events. Gerstein invited ICE to attend the OpEx events and to nominate topics.

15. **PUBLIC COMMENT:** There were no comments from the public.

16. HSSTAC FEEDBACK AND INITIAL RECOMMENDATIONS

Gerstein left committee members alone to discuss what they had heard. He returned an hour later and asked members for their perspective.

Homeland Security Science and Technology Advisory Committee (HSSTAC) Chairman Phil DePoy commented that the meeting structure, especially the focus on components, was successful; however, the focus remains mostly tactical. He also suggested that the role of the centers of excellence (COE) should be reexamined for possible re-focus on the future.

- Gerstein responded that the dialogue is shifting toward a long-term focus. Two components have asked for help thinking about the future (10 years out), and he plans a year-long, \$1-million-dollar “futures” study. He added that this was the main purpose of the recent focus on broader roadmaps (vs. a “project-by-project” focus).

- ICE Liaison to S&T Cloe Vincent commented that today’s discussion was limited due to the open forum. She added that ICE does not have a “Research and Development (R&D)” office; however, it does have a R&D advisory group.

Committee Comments About S&T-ICE Relationship:

- There is no unified, integrated strategy with ICE (same thing as last meeting with Customs and Border Protection (CBP)).
- Briefs should begin with a focus on ICE needs in future, at least five years from now.
- ICE’s problems center on the human element and social networks, but DHS S&T is focused largely on the technologies. The balance is not quite right.
- We heard too many sales pitches from S&T to ICE. Next time, include failures too.
- The strategic value of the virtual shooter isn’t clear.

General Committee Comments:

- DHS S&T should clarify what it wants from its advisory committee.
- The meeting exceeded my expectations regarding the deep knowledge and range of activities.
- The meetings have improved regarding useful information communicated.
- DHS S&T is better linked with components; now it’s time to go beyond tactical to strategic.
 - Gerstein commented that DHS S&T is the lead for the DHS Joint Requirements Council which addresses several topics, including cyber, biodefense, common vetting, borders, and multi-role mission aircraft.
- Components seem to be working with each other more—and DHS S&T is working across components more. This is a positive direction.
- You may need a different type of systems analysis.
 - Gerstein commented that DHS S&T is moving in that direction and is trying to build a workforce that can handle a “systems” approach.
- Operational security may be limiting what is shared with the committee, impeding the members’ ability to understand the issues and give its best advice.
 - Gerstein reminded members of Federal Advisory Committee Act (FACA) requirement for openness and reminded them of the closed session on Day 2.
- It isn’t clear that you have the right centers of excellence (COEs) or that they are being leveraged as well as they could be; consider a scientific evaluation of the COEs.

- You need a threat roadmap. This seems to be a DHS-wide issue.
- Drones may be the biggest problem of the 2nd half of 21st century.
- Social media issues will increase, and a lot of threats come through social media. You may need a unified strategy, including threat tracking. Consider doing an analysis of the social infrastructure and how it impacts components. S&T could step into this space for DHS.
 - Gerstein acknowledged that other organizations are ahead of DHS in this area. DHS S&T is leading Big Data for the department but could do more with social media.
- Every component has a human infrastructure outcome. In a law enforcement culture, it can be very hard to understand how the human element affects them.
- Share your busts too. If you don't have busts, you're not pushing the envelope enough.
- Let's hear what you have learned from mistakes. You need the luxury to make mistakes. Encourage truth-telling and don't penalize people for it.
 - Gerstein mentioned Secure Transit Corridor is an example of this success/failure issue. Customs and Border Protection (CBP) decided not to pick it up, and it lacked a systems approach. He added that DHS S&T is moving toward more technical risk, but it requires component buy-in.

17. HSSTAC WAY AHEAD

Gerstein gave an overview of the Integrated Investment Life Cycle Threat (IILCM), indicating a number of projects failed due to the lack of process. He discussed the proposed stand-up of the Joint Requirements Council (JRC), Resource Allocation Decisions, and the Department of Defense (DoD) process known as "DOTMLPF" (Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities). He added "R/G/S" (Regulations, Grants, and Standards) to the DOTMLPF as part of the necessary process. He emphasized he does not want to build a DoD-like acquisition process, but rather wants a process that is agile and nimble.

ADJOURN: **Gerstein** adjourned the meeting at 4:13 PM.

April 8, 2014

1. CONVENE/OPENING COMMENTS

DHS S&T Under Secretary (Acting) Daniel Gerstein reconvened the meeting at 9 a.m. and reviewed the agenda.

2. UPDATE AND DISCUSSION: CYBER SECURITY DIVISION

(For related slides, go to <http://www.dhs.gov/st-hsstac>. Scroll to "Past Meetings," then "April 7-8, 2014." Select "Meeting Briefs." Then select "HSSTAC Cyber Brief - April 08.")

Doug Maughan, Director, Cyber Security Division (CSD), Homeland Security Advanced Research Projects Agency (HSARPA), DHS S&T reviewed the history of cyber security, including the creation of the division in 2010, and the interaction with the Homeland Security Science and Technology Advisory Committee (HSSTAC) from July 2008 to today. He showed how the cyber security budget at S&T has grown from \$3 million in FY03 to \$70 million in FY14. He reviewed HSSTAC's report on cyber security (December 2008), including its findings and recommendations. He also reviewed briefs that he previously shared with HSSTAC members -- in 2008, 2010, 2011 and 2013. He discussed the current state and future projections for CSD, including current cyber threats and sources, White House priorities, the organization of the U.S. Federal Cybersecurity Operations Team, a recent Executive Order and Presidential Policy Directive, and current cyber security thrust areas. He reviewed resource allocations and key partnerships. He described the transition goals and cyber-physical systems. He then listed ideas for new programs, described 2014 plans for Broad Agency Announcements (BAAs), and described the execution model for cyber security R&D. He summarized by emphasizing S&T's aggressive cyber security research agenda, continued emphasis on technology transfer and experimental deployments, and workforce concerns. Regarding HSSTAC's interactions with CSD over six years, he commented that the quality has been excellent and helpful—but the interactions have been too few. In future, he prefers more frequent interactions and deeper cybersecurity knowledge. He suggested that the Homeland Security Science and Technology Advisory Committee (HSSTAC) consider re-establishing topic-specific subcommittees or working groups in order to enable better technical interactions. He added that another written report from HSSTAC on this topic may be useful.

A discussion followed regarding organizational resilience to cyber attacks, the nexus of social media with federal cyber security, lanes of responsibility, the difficulty of attracting industry proposals, and how HSSTAC can best support CSD in the future.

Committee member comments:

- HSSTAC needs a true cyber expert as a member.
- HSSTAC should create a standing subcommittee or task force of cyber experts.
- The former HSSTAC Subcommittee on Cyber Security supported the division, but never briefed the full committee or the Under Secretary.
- CSD invites formal feedback, but S&T has steered away from formal HSSTAC reports.
- Consider creating a center of excellence specifically for cyber security.
- Consider creating a federal advisory committee just for this subject.
 - Maughan explained that DHS's National Protection and Programs Directorate (NPPD) asked for a committee focused on cybersecurity, but it was not approved.

3. S&T PROJECT BRIEFS: APEX AIR ENTRY/EXIT RE-ENGINEERING PROJECT

(For related slides, go to <http://www.dhs.gov/st-hsstac>. Scroll to "Past Meetings," then "April 7-8, 2014." Select "Meeting Briefs." Then select "HSSTAC Apex AEER Brief - April 08.")

Bob Burns, Apex Program Manager, Homeland Security Advanced Research Projects Agency (HSARPA), DHS S&T explained that Apex is a concept, not a division, and that

Apex projects are hard-hitting, fast-moving, and based on component input. The Air Entry/Exit Re-Engineering Project (AEER) is the 4th Apex project. AEER is a joint effort between Customs and Border Patrol (CBP) and DHS S&T to more efficiently identify travelers entering the U.S. while biometrically confirming the departure of non-U.S. citizens. He explained its goals and objectives, framework, drivers, and timeline. He described the Maryland Test Facility (MdTF) to test biometric technologies and other processes. An open house at MdTF is planned for June, and the public will be invited, he said. He listed results so far, next steps, and challenges. He invited committee input during project execution.

A discussion followed with HSSTAC members concerning the driver for this project (biometric identity is required by Congress beginning in 2019); whether other countries' entry records could serve as U.S. exit records, and how privacy laws may limit such sharing; Singapore's and Malaysia's success in this area; how conditions in the U.S. differ from those in other countries (for example, the U.S. has more international airports); the potential economic impact on airlines and airports; the human factors inherent in this program; the business case and trade-offs; and the balance between convenience and security.

S&T PROJECT BRIEFS: PROJECT RESPONDER 4

(For related slides, go to <http://www.dhs.gov/st-hsstac>. Scroll to "Past Meetings," then "April 7-8, 2014." Select "Meeting Briefs." Then select "HSSTAC PR4 Brief - April 08.")

Jose Vazquez, Director, Responder Technologies, First Responder Group (FRG), DHS S&T explained why a project focused on first responder needs is necessary, described the predecessors for Project Responder 4 (PR4), and explained its purpose and objectives, terminology, methodology, and phases. He explained three ways that PR4 identifies capability needs and listed capability priorities. He then explained PR4's response technology objectives (RTOs) and the four-step process to identify them. He explained the expected products and showed an initial roadmap for the developing the RTOs. He emphasized that FRG works with first responders from beginning to end to clarify conditions and requirements, and acknowledged the need to better integrate different technologies. He added that he is now addressing the role of social media and the need to assess its usefulness.

A discussion followed with committee members concerning the balance between long-term and short-term needs; public safety broad band; how FRG works with the Federal Emergency Management Agency (FEMA); the need for science to back resource requests; how to determine the right standards (driven by industry); and how to balance safety and efficiency.

4. **PUBLIC COMMENT:** David Oliver (Catalyst Partners) commented that at a time of low employee morale, it might help if the committee recognized successes at DHS S&T, in addition to recommending improvements.

5. CLOSED SESSION: EMERGING AND DISRUPTIVE TECHNOLOGIES AND TRENDS

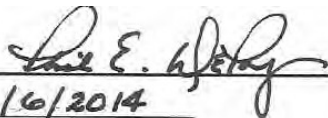
Joel Wall, Director, Special Projects Office, DHS S&T described the mission of his office to provide programmatic and technical expertise and knowledge in emerging and disruptive

technologies, Intelligence Surveillance and Reconnaissance (ISR), and other applicable areas that are especially sensitive, classified, or deserve extraordinary security protection; and how he accomplishes these objectives through close collaboration and leveraging with the Intelligence Community (IC) and other government agencies. He described related technology trends and special projects. (This session included classified information. Closure justification: 5 U.S.C 552b(c)(1))

6. CLOSED SESSION: HSSTAC TASK FORCE ON THIRD PARTY PRE-SCREENING

Homeland Security Science and Technology Advisory Committee (HSSTAC) Chairman Phil DePoy updated the committee on the progress of the task force which was created in July 2013 at the request of the Transportation Security Administration (TSA) to help TSA explore ways to expedite physical screening through the use of third-party (private sector) entities. Task force members were asked to help evaluate the feasibility of such an approach by reviewing testing and evaluation plans, and to provide input on evaluation criteria. DePoy emphasized that the goal is to improve air passenger through-put and lessen disruption to the public. He described responses to TSA's Request for Information (RFI). Discussion followed regarding privacy issues, databases, and risk classifications. (This session included sensitive security information (SSI) and confidential business information. Closure justification: 5 U.S.C 552b(c)(3) and 5 U.S.C. 552b(c)(4))

7. ADJOURN. Designated Federal Officer Mary Hanson adjourned the meeting at 3:00 p.m.

Signed :  (HSSTAC Chairman Phil DePoy)
Date: 6/6/2014

MEETING ATTENDEES

HSSTAC Members (April 7, 8):

Steven Bellovin
Kathleen Carley
Julie Casani
Phil DePoy
Dean Kamen (by phone, April 8 only)
Alex Levis
Mark Lister
John Parow
Yossi Sheffi

Members of Public:

Diana Fossett –Noblis, Inc. (April 7, 8)
David Oliver – Catalyst Partners (April 7, 8)
Jason VanSice - MorphoTrust (April 8)

DHS/ICE (April 7):

Daniel Ragsdale – ICE Deputy Director
Eric Feldman - Unit Chief, Cyber Crimes Investigations (C3), Homeland Security Institute (HSI)
Kelly Oliver - Section Chief, Technical Operations, HSI
Joshua Archer - Technical Operations, HSI
Bert Medina - Assistant Director, Office of Firearms and Tactical Programs
Thariq Kara - Program Manager, Office of Chief Information Office (OCIO)
Simona Flores - Deputy Asst. Dir. for Field Operations, Enforcement and Removal Ops (ERO)
Megan Davis - Deputy Chief of Staff, Deputy Director's Office (also April 8)
Cloe Vincent - ICE-S&T liaison (also April 8)
Jeremy Shein – HSI

DHS/S&T (except where noted):

April 7, 8

Mary Pickering (OCIO)
Mary Ellen Hynes
Alexandra Waggoner
Craig Chambers
Christopher Featherston
Mila Kennett
Joe Kowalski

April 7

Cecilia Grillo (NPPD)
Scott Tousley
Adam Cox
Jim Tuttle
Stephen Hancock
Stan Cunningham
Sonja Rodriguez
Christopher Lee
Joel Wall
Kathleen Kenyon
Jonathan MacEntee
Heidi Whiteree
Scott Pugh
Richard Williams
Doug Lane
Marck Kaczmarek
Douglas Maughan
Ryan Haddad
Christopher Lee
Steve Dennis
Jamie Johnson
Joseph Scott
Keith Holtermann
Susan Law
Greg Price
David Throckmorton
Linda Vasta
Jessica Augustine
Megan Mahl
Phil Waters
Rolf Dietrich
Brendan Gibbons
Bruce Swlc (signature intelligible)
April 8
Kentia Elbaum (DNDO)
Craig Chambers
Meredith Lee
Colette Bryant
Arun Vemury
Dayo Simms
Anneke Baran
Hyuen (signature intelligible)
Mark Cal (?) (signature intelligible)
Siddha Horer (?) (signature intelligible)

**Department of Homeland Security (DHS) Science and Technology Directorate (S&T)
Homeland Security Science and Technology Advisory Committee (HSSTAC)**

**December 4 -5, 2013
1120 Vermont Ave. NW
Washington D.C. 20005**

MEETING MINUTES

December 4, 2013

Summary: About 40 people attended, including six committee members, eight representatives of Customs and Border Protection (CBP), and 24 members of the public. (See list at end.)

1. CONVENE AND INTRODUCTION TO DHS S&T

Acting Under Secretary for S&T Daniel Gerstein convened the meeting at 8:55 a.m. He explained that he wants feedback on how S&T is supporting the components and invites the committee's ideas in this regard. He noted that S&T is focused more on capabilities. He explained that this meeting will test a new methodology for HSSTAC which focuses on DHS components. He then provided an update on S&T, explaining that it brings key technical and analytical capacity, is operationally focused, and has its own labs. He emphasized that S&T is not only about technology but also process enhancements and business reforms.

STRAS Overview

Gerstein explained the new Science and Technology Resource Allocation Strategy (STRAS) process (slides #26-30), through which S&T will ask components about their capabilities and gaps and will then use their input to generate a "signature document." The signature document will help S&T and the component reach agreement on a schedule for all phases of development projects. **Gerstein** announced that the 2nd day of this meeting will represent the pilot of this process with CBP. **Gerstein** and the HSSTAC members then discussed the documentation requirements, competing requirements, and the decision-making process.

HSARPA Overview

Adam Cox, Acting Director of the Homeland Security Advanced Research Projects Agency (HSARPA), briefed the committee on HSARPA's role and mission (slides #34-55). He explained that HSARPA is moving toward more consistent metrics and is considering new ways to use BAAs and "term" Program Managers to facilitate creativity. He then briefed the committee on the missions of each HSARPA division and discussed S&T's two current Apex projects: AEER (Air Entry/Exit Re-Engineering) and BEAP (Border Enforcement Analytics Program).

FRG Overview

Jay Martin, Deputy Director of the First Responders Group (FRG), briefed the committee on FRG's role and mission (slides #56-85), noting that FRG has a broad constituency. He then gave an overview of the five FRG divisions, noting that FRG is a small part of S&T's R&D budget, with the majority allocated to technology development. He explained how FRG developed its foundational document by partnering with FEMA to commission a report which defined 40 broad capability areas. He explained that the First Responders Resource Group (FRRG) helps to develop operational requirements. He noted that travel restrictions have reduced FRG's ability to do outreach and engagement, and remote options do not adequately fill the gap. He explained FRG's process to identify needs (slide #69), and that technology foraging is a key element in solving them. Martin and the HSSTAC members then discussed examples of FRG-funded technologies, the acquisition process, and the need to measure impact and investment.

ASOA Overview

Debra Durham, Director of the Acquisition Support Operations and Analysis (ASOA), briefed the committee on ASOA's role and mission (slides #86-112) and explained how S&T leverages enterprise architecture that is managed by DHS operations. She noted that the ASOA budget has decreased, along with the early emphasis on standards. She explained its oversight of S&T's two Federally Funded Research and Development Centers (FFRDCs) and its focus on analysis of alternatives (AOAs) and transition. She highlighted the Rio Grande Valley (RGV) project with CBP. Durham and the HSSTAC members then discussed systems integration, components' ability to analyze their needs, the development and application of standards, and the management of the Transportation Security Lab (TSL), which is TSA's designated test authority. Durham highlighted ASOA's first systems analysis guidebook, which standardizes process and steps and is available to the public (slide #95.) **Gerstein** interjected that S&T has developed more than 250 knowledge products since the last HSSTAC meeting (slide #110).

RDP Overview

Keith Holtermann, Director of Research and Development Partnerships (RDP), briefed RDP's mission and goals (slides #113-131) and explained how RDP fosters collaboration across the government, creates and manages partnerships, and provides a bridge between internal partners and external ones. He noted that most of RDP's budget goes to the Office of National Labs (ONL) in direct support of the labs, and emphasized that RDP has equal access to the DOE labs. Holtermann and the HSSTAC members then discussed S&T's engagement with labs (including DoD's and HHS's), international and interagency engagements, and the Joint Interagency Field Experiments (JIFX).

2. BRIEF: DHS S&T RESILIENT SYSTEMS DIVISION (RSD)

RSD Division Director Jalal Mapar briefed on S&T's newest division (slides # 132-159), which was formed in 2012. He explained that resilience cuts across many disciplines and its definition varies. He described how he used a systems approach to build the division and defined the attributes of resilience (slide #136) in order to build a framework. He described

RSD's thrust areas (slide #140) and the objectives under them. He emphasized the need to focus on end users, and to work closely within S&T and with DHS components regarding end-user requirements. He emphasized the need to increase the speed and effectiveness of disaster response and to reduce recovery times, and highlighted areas where RSD efforts can make a big impact. **Mahar, Gerstein** and the HSSTAC members then discussed RSD coordination with other divisions, how it leverages work by others, the emphasis on and difficulties surrounding transition, and the development of best practices and roadmaps.

3. DISCUSSION AND FEEDBACK

HSSTC members commented on the importance of relationships with components and getting feedback from end users. They discussed outcomes and metrics, the complex environment of DHS, how to determine the value of S&T's work, the need for adaptability in the budget, and the need for a strategic element. Members applauded the closer relationship with components and the increased emphasis on an operational and systems approach. They suggested a better feedback loop for user impact, a possible market analysis, better metrics for success (especially regarding knowledge products), and possible cross-cutting themes.

4. STATUS REPORT: HSSTAC TASK FORCE ON THIRD PARTY PRE-SCREENING

Task Force Vice Chair Brian Toohey briefed the committee on the task force which was created under HSSTAC in July 2013 to advise TSA in its goal to make travel both safer and more convenient, possibly by using industry to facilitate passenger pre-screening. The task force has held two webinars and one full-day meeting. TSA invites task force input during the early stages of T&E, and also invites input about whether prototyping should be pursued. The task force plans to meet in early 2014 to develop recommendations regarding next steps. Toohey and the HSSTAC members then discussed the issue of threat identification, the potential impact of third-party screening on airport lines, and the task force timeline.

5. PUBLIC COMMENTS

Andy McDonald, BAE Systems, commented on DHS's acquisition process. An Army veteran with acquisition experience, he compared DoD's and DHS's acquisition history and noted that the two agencies are on some parallel paths. He suggested that DHS standardize and integrate its equipment, and team up with DoD when appropriate.

David Armour, Cypress International, commented on the impact of sequestration. He expressed concern that S&T's budget numbers may portray business as usual and may not show the impact of sequestration.

6. UPDATE AND DISCUSSION: INDUSTRY ENGAGEMENT WITH DHS S&T

Gerstein briefed the committee on S&T's industry engagement (slides #162-169), gave some examples of successful partnerships that led to transitions, and asked for discussion and feedback on the current S&T tools for industry collaboration. The discussion centered on competitions, the need to publish well-defined needs, how to find industry partners, how to communicate to industry that a market exists, and the role of industry in helping to transition technologies. **Cox** described how HSARPA has used webinars to communicate with industry and has tried to stimulate competitions through Broad Area Announcements (BAAs).

HSSTAC members suggested that S&T consider sponsoring an X Prize; be more explicit about needed capabilities and whether it is seeking a new capability or an improvement on an existing one; use other avenues besides FedBizOps; consider tapping the investment community; and consider business models that might help industry understand the market. **Gerstein** asked for input on how to find industry partners for the mid to late stages of a product and emphasized the hope that webinars would help to communicate the transition needs. HSSTAC members suggested talking to the customer base; the need to develop standards, which can require international buy-in; and the need for S&T to know its risk tolerance. **Gerstein** noted that connecting with industry partners is a key challenge for S&T.

7. HSSTAC WAY AHEAD

Gerstein announced that the second day of the meeting will focus on S&T engagement with Customs and Border Protection (CBP).

8. ADJOURN: Hanson adjourned the meeting at 4:30 p.m.

December 5, 2013

1. CONVENE AND BRIEF: CBP OVERVIEW AND TECHNOLOGY NEEDS

Acting Under Secretary for S&T Daniel Gerstein convened the second day of the HSSTAC meeting at 9:05 a.m. He reminded attendees that the over-arching goal for DHS S&T and for the HSSTAC meetings is to better perform the S&T mission, and HSSTAC will now focus its quarterly meetings on DHS components. Today's component of focus is Customs and Borders Protection (CBP).

Mark Borkowski, Assistant Commissioner for the Office of Technology Innovation and Acquisition (OTIA), explained the mission and roles of CBP, including as an economic driver. He described its operational context and technology needs. Discussion followed regarding technology readiness levels (TRLs) and the transition and acquisition process.

Colleen Manaher, Executive Director for Planning, Program, Analysis and Evaluation, Office of Field Operations (OFO), gave an overview of OFO's mission and challenges. Discussion followed regarding the impact of flat budgets, the need for more personnel, the need for partnerships (including with industry), the proper balance of security with privacy, the role of technology, and how to measure return on investment.

Andrew Scharnweber, Patrol Agent In Charge, Office of Border Patrol (OBP), explained OBP's risk-based strategies and the necessity to make choices under tight budgetary constraints. He emphasized partnerships and explained how technology can help agents, including for process improvement. Discussion with HSSTAC members followed regarding how requirements are collected, the pace of technological change, and CBP's use of gear that is redeployed from DoD.

Ron Reichel, Director, Requirements, Office of Air and Marine (OAM), described the OAM organization, missions, assets, and recent performance results. Discussion followed regarding the collection and analysis of data, how regional missions within OAM can differ,

the use of unmanned aerial vehicles (UAVs) and risk assessment models, a recent focus on hand-held devices to help agents on the ground, and the need for better surveillance.

Thomas Manning – Director, Collections Division, Office of Intelligence and Investigative Liaison (OIIL), described his office’s role and some recent enhancements in forensics, sensors, and predictive tools. He highlighted current S&T/CBP projects such as threat and anomaly detection models, and possible future collaborations such as space visualization.

Troy Riley, Executive Director, Commercial Targeting & Enforcement, Office of International Trade (OT), described OT’s operational environment as it works to move legitimate trade quickly while interdicting illegal flows, and emphasized the need to keep up with changes in the industry and technology. He described how commodities are organized and how data is managed. Discussion followed regarding cyber security and the support that OT receives from the DHS S&T Centers of Excellence.

2. HOW S&T SUPPORTS CBP

Dan Gerstein explained that all four groups in S&T support CBP and offered some budget numbers. He emphasized S&T’s desire to be operationally-focused while remaining innovative, which requires a good understanding of component needs. He emphasized the need for better lines of communication.

Adam Cox, Acting Director, Homeland Security Advanced Research Projects Agency (HSARPA), briefed on HSARPA engagement with CBP (slides #20-34). He gave an overview of HSARPA’s operational setting and budget environment, described specific projects that support CBP, and highlighted HSARPA’s interest in new technology development, in-depth assessments of commercially-available technology, and prototype development. A discussion followed regarding HSARPA’s relationships with components generally (and CBP in particular), how new technologies are tested, the rate of technology transfer, and the need for cyber security. **Cox** then described the HSARPA portfolio of 21 current CBP projects (slide #24).

Jay Martin, Deputy Director, First Responder Group (FRG), gave an overview of FRG projects that relate to CBP (slides #35-45), emphasizing that the tools are generally available to first responders.

Debra Durham, Director, Acquisition Support and Operations Analysis (ASOA), described ASOA links to CBP (slides #46-55), emphasizing the Rio Grande Valley (RGV) Systems Analysis. Discussion followed regarding how quickly the recommended changes are implemented, whether improvements were realized, the impact of cost, who has responsibility for testing, and whether a need exists for doctrinal solutions, training, or a cost-benefit analysis.

Keith Holtermann Director, Research and Development Partnerships, explained RDP as the support entity which facilitates the other work of S&T through partnerships (slides #56-63). He then reviewed RDP projects of interest to CBP.

Gerstein asked if there were any surprises in the preceding presentations. CBP representatives responded that there were none. This segment of the agenda concluded with a consensus that communication and cooperation between CBP and S&T has improved and should continue to increase. **Gerstein** emphasized that the STRAS process will be the tool to improve cooperation.

3. PUBLIC COMMENT

Ella Schiralli, Manager, Federal Government Markets, 3M Identity Management, emphasized the importance of partnership and engagement with industry; the sooner industry is brought into the loop, the better it can add effectively to the conversation

4. DHS DIRECTION TO HSSTAC

Gerstein asked HSSTAC members to discuss what they had heard during the two days of meetings and present their initial input to him in an hour.

5. HSSTAC FEEDBACK AND INITIAL RECOMMENDATIONS

Members held a one-hour working session to develop an out-brief to S&T and then presented their input to Dr. Gerstein. They applauded the format of the meeting and the evidence of closer links between S&T and CBP, and recommended that HSSTAC meetings continue the focus on DHS components but perhaps include a more strategic element in the future. Regarding CBP, they suggested that S&T consider developing a cyber strategy for CBP, and suggested that CBP operators may benefit from more engagement with S&T's technology foraging efforts. They also recommended that S&T continue to pursue better metrics of success and consider academic research beyond the DHS S&T Centers of Excellence.

6. ADJOURN: Hanson adjourned the meeting at 4:30 p.m.

Certified by: Phil DePoy (HSSTAC Chairman Phil Depoy) **Date:** 4 MARCH2014

MEETING ATTENDEES

HSSTAC Members:

1. Steven Bellovin
2. Kathleen Carley
3. Julie Casani (Dec. 4 only)
4. Phil DePoy
5. Mark Lister
6. John Parow

DHS/CBP: (Dec. 5 only)

1. Mark Borkowski – Asst. Comm. for Office of Technology Innovation and Acq. (OTIA)
2. Colleen Manaher – Exec. Dir, PPAE, Office of Field Operations (OFO)
3. Thomas Manning – Dir., Collections Division, Office of Intel. and Inv. Liaison (OILL)
4. Troy Riley – Exec. Dir., Comm. Targeting & Enf., Office of International Trade (OT)
5. Ron Reichel - Director of Requirements, Office of Air and Marine (OAM)

6. Rick Dorsey - Program Manager, Office of Air and Marine (OAM)
7. Andrew Scharnweber - Associate Chief, Office of Border Patrol (OBP)
8. Jennifer Pennese – Dir., Strategic Transformation Office, Office of Field Operations (OFO)

Members of Public:

December 4, 2013:

1. John McGowan - Sandler & Travis Trade Advisory Services
2. Ella Schiralli – 3M Identity Management
3. Eric Juttelstad – Morpho Trust
4. David Olive – Catalyst Partners
5. Andrew Jay MacDonald - BAE Systems
6. Dave McWhorter – Catalyst Partners
7. Irelene P. Ricks - American Assn. of State Colleges and Universities, Grants Resource Ctr.
8. Paul Brenner - ICF INTERNATIONAL
9. Jesse Rauch – HP Autonomy
10. David T. Armour - Cypress International
11. Diana Fossett – Noblis
12. Andrea C. Marsh - Battelle Memorial Institute
13. Barbara Zalinsky – Implant Sciences Corporation
14. Kevin Brenker – Symetrica Inc.
15. Tarry Kirkland – SAIC
16. Joseph Gresenz – Battelle Critical Infrastructure Business Unit
17. Rick Muntz –Arktix Radiation Detectors, Ltd.
18. Rico Chandra – Arktis
19. Caroline Eliaser - P66
20. Margaret Goldberg – Noblis

December 5, 2013

1. John McGowan (see Dec. 4)
2. Ella Schiralli (see Dec. 4)
3. David Olive (see Dec. 4)
4. Andrew Jay MacDonald (see Dec. 4)
5. Dave McWhorter (see Dec. 4)
6. Paul Brenner (see Dec. 4)
7. David T. Armour (see Dec. 4)
8. Kevin Brenker (see Dec. 4)
9. Joseph Gresenz (see Dec. 4)
10. Diana Fossett (see Dec. 4)
11. Michael Butler - Deloitte Consulting, LLP
12. Robert Jacksta - Deloitte Financial Advisory Services, LLP
13. Shaq Sontakke - Deloitte Consulting, LLP
14. Andres Rodriguez – Wire Media

NOTE: Meeting materials are posted at <http://www.dhs.gov/st-hsstac>.

**Department of Homeland Security (DHS) Science and Technology Directorate (S&T)
Homeland Security Science and Technology Advisory Committee (HSSTAC)**

September 27 – 28, 2012
1120 Vermont Avenue, NW
Conference Room 5-212
Washington, DC 20005

MINUTES

Summary: About 35 people attended the inaugural session of the reconstituted HSSTAC, including 9 committee members and 7 members of the public. (See Attendee List, Page 11/12).

September 27, 2012

1. CONVENE AND INTRODUCTION TO DHS S&T

HSSTAC Executive Director and Designated Federal Officer Mary Hanson convened the meeting at 9 a.m. and read a statement regarding conflicts of interest. She added that members of the public were present.

Under Secretary for S&T Tara O’Toole welcomed committee members to the inaugural session and thanked them for their service. She explained that their interaction and collaboration with herself and other S&T staff would focus on their expertise and experience, and is intended to guide and develop the growth of the Directorate through their advice on a variety of levels—technical, strategic, policy, and so on. She highlighted the importance of their input and their role in improving S&T’s mission effectiveness.

O’Toole then briefed the members on the background and mission of S&T—which she described as the science and engineering core of DHS—and its relationships with DHS Components and other stakeholders. She explained the size and diverse nature of DHS and the operational nature of Components, many of which are not technically oriented or familiar with the role or function of research and development (R&D). She emphasized that strategic goals must be considered within the context of operational reality. She delineated the missions and focus areas of DHS and the importance of facilitating secure trade, travel, communication, etc., while also providing resiliency in the face of major incidents. She then discussed the value of S&T to DHS Components and stakeholders; for instance, to help improve efficiency and operational effectiveness; save lives, time, and money; and provide long-term return on investments (ROI). She emphasized the importance of partnerships with Components, especially their leaders and operators. She emphasized S&T’s unique bio-defense responsibilities and its role as R&D funder for civilian cyber security. She explained that at a more strategic level, she wanted to help incorporate systems engineering and analytical processes into DHS decision-making—a key area for committee advice. Finally, she gave an overview of budgetary challenges, pointing out that S&T receives about \$1 billion out of \$54 billion dollars allocated to DHS. She highlighted the significant cuts to research and operations budgets in recent years and described this trend as “unsustainable.”

2. DHS S&T STRATEGY AND PROCESS – DAN GERSTEIN

Deputy Under Secretary for S&T Dan Gerstein gave more details on the role of S&T and its relationships with DHS Components, interagency partners, and state, local, tribal, and territorial (SLTT) stakeholders, as well as its role in the international arena and its involvement with academia and the private sector. He described the role of S&T as “larger than delivering technology.” He emphasized the need to be operationally focused and innovative and to build partnerships. He explained that S&T’s mission guidance was built around an analysis of threats and challenges, ranging from tactical difficulties facing first responders to full-scale national emergencies. He noted that S&T’s mission directly supports a variety of Homeland Security Presidential Directives (HSPDs) and involves customers or partners across government mission areas, such as Critical Infrastructure and Key Resource (CI/KR) management and law enforcement. He mentioned the 53 percent “real reduction” in S&T’s budget from FY10 to FY12. **Casani** asked about allocations between discretionary and non-discretionary R&D. **Gerstein** explained that much discretionary funding focuses on R&D through university Centers of Excellence (COEs), partnerships with national labs, and efforts led by the Homeland Security Advanced Research Projects Agency (HSARPA). He pointed out that many DHS Components focus on policy or operational issues, and S&T needs to lead in the R&D arena. He emphasized again the importance of partnerships and operational relevance. S&T could help alleviate budgetary concerns, he said, by focusing on late stage technologies, successful transition and commercialization efforts, and reducing projects with less likelihood of success. **Carrano** asked about the effects of recent budget cuts and mentioned the importance of disruptive technology as an equalizer. **Gerstein** agreed that this is a key area to pursue, adding that tech foraging has also proven effective. He added that S&T is trying to help Components to develop requirements and invited HSSTAC input in this area. **Gerstein** closed his remarks by observing that S&T had experienced a number of challenges but also some successes, such as the development, with COEs, of a vaccine for Foot and Mouth Disease (FMD). **Levis** asked about the nature of resiliency and its role in the attack chain. **O’Toole** explained that resiliency as a goal is still developing and had been recently adopted across several agencies. She noted that its definition is still somewhat ambiguous and suggested this could be a good area for committee study.

3. ALL ABOUT S&T

HSARPA OVERVIEW – PAUL BENDA

Paul Benda, Director of the Homeland Security Advanced Research Projects Agency (HSARPA), briefed the committee on its role and mission. He explained that HSARPA is the primary source of innovation for the Department but should not necessarily be compared with the Defense Advanced Research Projects Agency (DARPA), since the latter had a much larger budget and a more integrated and established system to identify and transition projects. He pointed out that because of its varied stakeholders, HSARPA has to work with disparate levels of readiness and understanding. Successful transition is an ongoing challenge, he said, and a key reason that S&T is pursuing partnerships with the Components— to help ensure that S&T is working on component priorities and to position technologies for market adoption. HSARPA had experienced changes in recent years, he said; it is now less focused on basic research and more on transition and partnering, aiming to help Components do their jobs better, faster, and cheaper. S&T also wants to help increase its stakeholders’ technical prowess through education, he said, and eventually become a science and technology

clearinghouse for the Homeland Security Enterprise (HSE). **Casani** commented that this is a significant mission and could be cumbersome or risk mission creep, noting that best practices or legal issues might be outside the scope of S&T's responsibilities. **Benda** responded that advice could be tailored to specific needs and argued that if S&T didn't provide this information, stakeholders may need to reinvent the wheel or rely on vendor-driven information. **O'Toole** explained that S&T is designated by statute as the source of best practices for science and technology for first responders. She agreed that S&T should focus on missions and capabilities that are aligned to its priorities. Further discussion between **Casani, Griffin, Carrano, and O'Toole** addressed the extent to which S&T could achieve this while maintaining objectivity, and the proper roles and responsibilities of state and local governments in decision-making and prioritizing. **Benda** emphasized that HSARPA's ultimate goal is to impact stakeholder operations, but it could be somewhat agnostic regarding how that occurred. S&T doesn't seek to sell a particular program or project, he added; its partners can determine the best solutions and practices for their needs. He added that S&T is broadly focused on certain areas of national interest, such as biological detection and response, cyber security, explosives, and CI/KR – but stakeholder buy-in is critical to successful transition and deployment. The portfolio review process is one means to develop and guide successful efforts, he said, and has been helpful in defending budgetary choices to Congress. **O'Toole** offered some examples of CI/KR-related projects that had been re-directed or dropped after the portfolio review process, often due to concerns about transition or commercialization. **Carrano** mentioned the importance of systems engineering and the need to consider potential challenges such as training or budget issues. **Benda** agreed and emphasized the need to understand context and operational requirements of any project.

FRG OVERVIEW – BOB GRIFFIN

Robert Griffin, Director of the First Responder Group (FRG), briefed the members on the background, efforts, and challenges facing the FRG and the unique nature of its diverse and widespread stakeholders, who collectively incorporate thousands of systems, best practices, and operational requirements. Given this stakeholder base, he said, it is critical for FRG to work on areas of common concern across the first responder community (FRC), especially communications, data sharing, and responder safety and effectiveness. He observed that training and budget issues are a significant concern across this base, and any technical solutions fielded by FRG should be user-friendly and affordable in order to ensure consistent and long-term use. **Griffin** described the FRG as four groups focused on different areas of responsibility, working with each other and with laboratories to build technical solutions to operational problems that are solicited from the FRC. As an example, he described how FRG has coordinated with the Department of Agriculture and the California Department of Forestry and Fire Protection to improve the design of firefighter gear. **Carrano** asked about the role of disruptive technology. **Griffin** responded that the challenges in this area are partly the result of FRC culture and habits, and added that FRG needed to help the FRC adjust to potential game changers as they arise.

ASOA OVERVIEW – DEBRA DURHAM

Debra Durham, Director of Acquisition Support and Operational Analysis (ASOA), explained its mission to guide the analytics, systems engineering, and testing and evaluation within DHS. She emphasized the need to tie together the development activities of DHS Components and to include the perspective of the operational end-user. She noted that ASOA has worked extensively with Federally Funded Research and Development Centers (FFRDCs) and is working to develop models to assess and analyze risks across DHS. **O'Toole** pointed out that this is a new and important part of S&T's mission, and that systems engineering had not been pursued before, to this degree, within DHS. She invited HSSTAC advice on how to leverage limited resources to make DHS more systems-based and analytical. **Durham** added that ASOA has partnered with the National Institute for Standards and Technology (NIST) and with COEs, and is working to provide assessments and information to the FRC and other stakeholders. **Depoy** asked about the size and budget of the primary FFRDCs. **Durham** responded that the Homeland Security Systems Engineering Development Institute (HS SEDI) handles about \$100 million worth of projects, and the Homeland Security Studies and Analysis Institute (HSSAI) manages about \$30 million. She added that ASOA's stakeholders are also diverse and span the breadth of the HSE, making data-driven analytics and data integration even more important. She added that this could be a critical area for HSSTAC study. **Levis** asked about transition and transformation goals and how they differ from DoD's. **Lister** interjected that he was impressed by the extent of S&T's efforts here, and also wondered how S&T's efforts differ from DoD's. **Durham** responded that ASOA partners with other agencies as needed and was working out the transition process.

Note: The RDP Overview was delayed to the afternoon because of a scheduling conflict.

DISCUSSION – WHAT KEEPS YOU UP AT NIGHT?

Griffin began the discussion by describing his key challenges and the need to resolve them or mitigate their impact. He highlighted the need to consider the overall capacity of the HSE and its response capacity, especially given the FRC's vast requirements and scarce resources. He wondered how to increase the lifespan and efficiency of equipment and how to continue to "break into" the community and address its needs. He pointed out that the complexities of the FRC bring unique challenges to the management, coordination, and guidance of solution development. He added that it is difficult – but critical – to forge relationships with FRC leaders who can make decisions regarding budgets, policy, and transition.

Gerstein noted that cyber security is a major area of concern, especially since DHS is responsible for protecting the .com domain. He added that "big data" and requirements are his other areas of concern. A lack of analytical rigor or proper understanding of requirements is often enough to sideline or terminate a project, he said. He mentioned the convergence of technologies, which can give "state-like capabilities to non-state actors." He wondered how to balance the process of innovation with a linear process like systems engineering.

Benda spoke about the difficulty and complexity of operating within DHS. He said the department is blamed for every problem or perceived failure throughout the interagency, leading to a risk-averse culture which makes it difficult to make quick decisions or to attract innovative staff. From a threat perspective, he said he was concerned generally about the ability to respond

to more than one major attack—but more specifically about cyber and biological attacks. Those risks are complicated by ambiguous roles and responsibilities within the SLTT, he added.

Durham identified two primary areas of concern; internal communication stovepipes and the proper alignment of resources against requirements. She noted that her concerns may be somewhat unique since ASOA is relatively new and still evolving.

O'Toole identified people and processes as her first concern, commenting that it is difficult to attract and retain effective personnel. Strong engineers and scientists are critical to the S&T mission and need to also be placed in DHS Components, she said; however, this is made difficult by a confluence of events, including decades of criticism or devaluing of government service and a challenging personnel management system. It is also important to improve S&T's standing within DHS and the broader interagency, she added; R&D seems to be under-valued across the government and is vulnerable to budget cuts. **Kamen** commented that he views personnel as a primary issue which should be addressed immediately. **Bellovin** observed that retaining the right people seems to be a challenge across the government. **O'Toole** agreed with their assessments and reassured the committee that S&T staff are motivated and focused on the mission. She added that the committee could provide value by highlighting this concern to others. Discussion continued about this issue among **Carley, Casani, Carrano, Levis, Lister** and **O'Toole** as they considered various ways to address human resources, staff retention, and organizational culture.

ALL ABOUT S&T (CONTINUED) – RDP OVERVIEW - DAN GERSTEIN

Dan Gerstein, Acting Director of Research and Development Partnerships (RDP), explained that RDP has helped grow S&T's value within DHS by fostering coordination and innovation between S&T and a variety of organizations such as the Department of Energy (DOE) and its labs. Increased collaboration among laboratories has resulted in an increased focus on biological threats, he said, and S&T is now working to support customers across the breadth of bio-defense. He added that inroads have been made with interagency partners such as the defense and intelligence communities. **O'Toole** explained that S&T's labs are managed by different entities and handle classified information, which makes it difficult to partner with universities. **Gerstein** pointed out that DHS has worked extensively with universities and has sponsored a network of 12 university COEs which he called “very entrepreneurial.” **O'Toole** added that the COE program has existed for nearly 10 years and is showing significant results, highlighting the importance of long-term relationships. **Gerstein** then discussed the role of other engagement methods, including Public-Private Partnerships (PPP), international partnerships, and long-range broad area agreements (BAAs.) **Lister** asked about BAA response rate. **Gerstein** responded that about 200 responses are received each year and emphasized that the long-range BAA is designed to solicit proposals on a rolling basis. He added that technology foraging is a key effort in RDP and helps reduce superfluous efforts and increase the efficiency of S&T and its partners. **Kamen** observed that it must be difficult for international partners to work with the U.S. government and asked how S&T manages this. **Gerstein** responded that, while it is a challenge, DHS does not differ much from other agencies in this regard. Discussion continued among **Lister, Gerstein, Kamen,** and **O'Toole** regarding strategies to ease these challenges, including the role of Other Transaction Authority (OTA) and the importance of fostering a culture of innovation.

4. HOW S&T WORKS (BUDGET) – DICK WILLIAMS

Dick Williams, the Chief Financial Officer (CFO) of S&T, gave an overview of the S&T budget and funding environment. He emphasized how little discretion exists in the R&D budget, which includes support to labs. Budget cuts have required S&T to prioritize and reduce projects from about 200 to about 60. The FY13 budget looks better, he said, but will be difficult to maintain. He emphasized that the budget environment calls for clear priorities.

5. DHS HISTORY AND OVERVIEW – KEN RAPUANO

Ken Rapuano, Director of Advanced Systems and Policy at MITRE Corporation, former Deputy Homeland Security Advisor to President Bush and former member of HSSTAC, gave a briefing on the creation, mission, and evolution of DHS and the challenges it faced in its first decade. He emphasized that there is no more complex mission space in the federal government than homeland security, noting that the traditional national security space is smaller and considerably more homogenous. He explained that DHS was formed following the 9/11 attacks to improve coordination and efficiency in preventing and mitigating significant threats to homeland security, and is now the third largest agency by budget and staff size, with a budget approaching \$70 billion in FY13. He described DHS goals and priorities as outlined in the Quadrennial Homeland Security Review (QHSR). He discussed the interagency coordination process, led by DHS, and executive branch processes for developing and coordinating the implementation of homeland security policies. He described the complexity of Congressional oversight of DHS, which is spread across many committees. He noted that efforts to define homeland security – both as an area of practice and as a policy issue – are ongoing and evolving. He highlighted the operational nature of many DHS stakeholders, particularly at the SLTT level, adding that the SLTT is often primarily focused on day-to-day issues and don't have the luxury to focus on lower probability/higher consequence risks for which DHS has an important responsibility. He emphasized the wide range of perceptions of risk in the homeland security spectrum, and how those perceptions drive dissimilar priorities for different stakeholders. **Carrano** commented on the spectrum of risk, from low probability/high consequence to high probability/low consequence, and observed that S&T seems to focus on one end of the spectrum but there isn't a need to choose. **Rapuano** responded that tension exists between SLTT and federal requirements, and that S&T has to balance its focus tactical as well as strategic requirements in its support to the FRC. He emphasized that 38 federal departments and agencies support emergency response and the coordination between these entities is complex and requires significant coordination to be effective. An understanding has evolved that not every threat can be mitigated, he said, and this understanding has led to a necessary focus on resiliency. A discussion ensued among **Carrano, Rapuano, Casani, Bellovin, and O'Toole** regarding thresholds of acceptable risks and acceptable consequences, and how to measure them. **O'Toole** highlighted the role that S&T has played in producing risk assessments for various threats and mentioned that S&T has a statutory responsibility to assess chemical, biological, radiological and nuclear (CBRN) risk. Committee members then discussed potential methods to analyze and respond to evolving scales of threat, and how to delineate roles and responsibilities for SLTT and federal entities. **Rapuano** ended by recommending that S&T build upon its current emphasis on taking a systems approach, by assessing the full 'threat chain' associated with different mission outcomes, to identify those areas where technology can provide the highest return on investment to achieving mission outcomes. As an example, he described how the Joint Improvised Explosive Device Defeat Organization (JIEDDO) evolved from its original focus on the point of explosion, by moving 'left of boom' to address the broader threat chain of activities and

associated signatures involved with IED attacks, to identify higher impact solutions focused on more on the root versus the symptoms of the problem. Information and systems integration are critical to success, he said. He emphasized the need to keep in mind the practical requirements and capabilities of end users.

Note: The HSSTAC Introduction and History was delayed to allow more time for discussion.

6. FACA BRIEFING – GEORGIA ABRAHAM

DHS Committee Management Officer Georgia Abraham briefed the members on the Federal Advisory Committee Act (FACA) and the operation of advisory committees. She discussed the roles, responsibilities, and restrictions of members of FAC committees. Committee members asked questions regarding the creation and conduct of subcommittees, justification for closing meetings, and requests to testify to Congress.

7. ETHICS BRIEFING – TROY BYERS

DHS Ethics Attorney Troy Byers briefed on the legal and ethical requirements of Special Government Employees (SGEs) who serve on FAC committees and the restrictions associated with that role. Committee members asked questions to clarify guidance regarding privileged information and the extent to which members can publicly declare their HSSTAC membership.

8. ADJOURN: **Hanson** adjourned the meeting at 4:30 p.m.

September 28, 2012

1. CONVENE: **Hanson** convened the meeting at 9 a.m. and read a statement regarding conflicts of interest. She added that members of the public were present.

2. HOW TECHNOLOGY CAN ADDRESS HOMELAND SECURITY CHALLENGES

O'Toole emphasized that she invites a range of inputs from HSSTAC, both formal and informal – possibly through a report to Congress, or specific reports on discrete issues, or subcommittees (for example, to advise TSA on the health effects of technology). She emphasized again the desire to drive DHS towards analytics and systems-oriented thinking, but also mentioned practical questions such as how to handle the budget environment. She explained that this session of the agenda would encompass three areas: innovation, emerging threats, and big data.

A. ECOSYSTEM OF INNOVATION

O'Toole pointed out that within the field of R&D, innovation is critical to maintaining relevance, breaking new ground, and ensuring ROI for stakeholders – and it involves more than technical ability. An innovative culture and strong partnerships with like-minded organizations could significantly improve the capabilities of the directorate over the long term, she said.

Carrano agreed with her assessment and observed that innovation involved not just the successful development of useful products or processes, but also the ability to ensure their widespread delivery and use. **O'Toole** noted that S&T is in a strong position to identify future

trends, given the scope of its mission and the breadth of its stakeholders and partners. **Bellovin** commented on the difficulty finding the right balance between innovation and partnerships, and the importance of recognizing cascading consequences and ripple effects. He added that partnering with industry is a key metric for success. **Depoy** noted that industry partnerships are often hindered by perceptions within the private sector that government partners may back out of a project or that their involvement may become burdensome. **O'Toole** responded that S&T has enjoyed success by working with In-Q-Tel (IQT) as a link to small and innovative organizations. Discussion continued regarding collaboration with industry, academia, and other partners among **Lister, Carley, Kamen, and O'Toole**. **Carley** commented that law enforcement needs to try out new technologies; the key, she said, is the technology infrastructure. **Kamen** mentioned the possibility of an "entrepreneur in residence" and described the role of urgency in driving innovation. **O'Toole** responded that operational urgency sometimes gets in the way of innovation at DHS. Discussion then turned to the importance of achieving large, notable successes. **Lister** mentioned the Apollo and Manhattan projects and observed that S&T could use similar but smaller victories to increase its visibility. **Kamen** commented that big organizations can innovate if they deem it to be critical; for example, DoD finds ways to address requirements rapidly when it is at war. **Carrano** mentioned that S&T needs to figure out how to market itself, which would lead to more successes and increased awareness. **Lister** asked if Components use a red team process, and **O'Toole** confirmed that some do. **Lister** recommended combining red teaming with systems engineering. **Gerstein** responded that the Rio Grande Valley project was based on challenges and requirements from Customs and Border Protection (CBP), and S&T is currently red teaming this project. **Lister** wondered if HSSTAC could help market or coordinate this area. **Gerstein** then mentioned working with Immigration and Customs Enforcement (ICE) on "big data," and **Durham** mentioned that ASOA is working with TSA on next-generation screening. **O'Toole** mentioned the danger of overreach and the need to work with those who are willing and able. **Lister** mentioned that in order to attract the right people and create a culture of innovation, S&T must provide problems that are hard, interesting and important. **Gerstein** mentioned that S&T is broadening stakeholder involvement in its portfolio reviews to help increase buy-in and interest. The committee then reexamined the issue of academic and private sector contributions to S&T, with a specific focus on how to attract the best and brightest innovators. **Carrano** suggested that S&T consider issuing a grand challenge with prize money as a way to incentivize industry. **O'Toole** responded that S&T does have the authority but it is difficult to achieve. **Kamen** mentioned that grand challenges have worked well within industry but it takes time and energy and is a budget challenge. He mentioned the successes of the X-prize and expressed a willingness to help S&T make inroads here if desired – but noted that he does not represent or advocate for it. **Levis** also noted that grand-prize challenges have had a degree of success within industry and academia, but emphasized that the prize should involve vision and not just gadgetry. **Kamen** mentioned the cost of security (especially infrastructure and airline security) and suggested that S&T could demonstrate cost savings by designing a better and more user-friendly system. He acknowledged that this is more of a policy issue than a scientific one, but the public trusts science so perhaps it could be used to influence policy decisions. Discussion continued among **Kamen, Levis, Benda, O'Toole, and Carrano** regarding strategies to engage partners, and using liaison officers or government exchange programs modeled after an academic sabbatical. It concluded with a general consensus that systems analysis and guidance throughout the innovation and transition process would be critical to mission success.

B. EMERGING THREATS

O'Toole opened this discussion by noting that emerging and future threats are often ambiguous and hard to quantify, and that this could be a key area of study for HSSTAC. **Gerstein** briefed the members on S&T's analysis of emerging threats and highlighted the metrics for gauging their scale, threat, and likelihood while noting that technology would play a key role in augmenting prevention or response. **O'Toole** said that one key area for potential HSSTAC focus is in biodefense and clarifying the roles and responsibilities of DHS and its interagency partners, especially DoD. **Gerstein** added that new technologies and practices had created the potential for widespread consequences of certain disasters or attacks—for example, Deepwater and Fukushima—and this is further complicated by the complex relationship between federal and SLTT levels. **O'Toole** commented on the continuing struggle to conceptualize preparations for large-scale catastrophes, given their cascading effects and other contingencies that are difficult to anticipate. At a strategic level, she said one of the primary challenges facing planners and policy makers is the need for situational awareness at all levels of government during a response. **Kamen** mentioned that the World Economic Forum addressed the issue of emerging threats. **Carley** mentioned that social media and other communications tools could prove valuable here, and **Levis** interjected that situational awareness and situational understanding are both critical to proper decision making and equally important. **Casani** agreed with **Levis** and observed that there is often no shortage of information; in fact, decision makers are often faced with an overload of data which needs proper analysis. **Gerstein** concluded the discussion by explaining the directorate's goals for the next QHSR cycle and by inviting advice in this area.

C. BIG DATA

Gerstein opened the conversation by offering questions and challenges, such as how to properly gather, analyze, and understand information and translate it into effective and timely decision-making. **O'Toole** mentioned that one enduring challenge is the need for situational awareness. **Durham** noted that “big data” is largely shaped by analytics and systems engineering, areas in which ASOA is taking a lead. She described ASOA's efforts to focus on the volume, velocity, variety, and trustworthiness of data, and understanding how data evolves during an incident. **Benda** highlighted the variety of areas where DHS could lead, adding that the vast scope and size of the department would require proper data integration and analysis. He referenced ongoing efforts with ICE as an example of success, and argued that S&T could help Components and partners streamline their analysis processes. **O'Toole** mentioned a randomization algorithm, developed by a COE and used by USCG patrols, as an example of that. **Carrano** described the “big data” challenge as a need to synthesize, analyze and filter. **Carley** mentioned an upcoming report from National Academy Press about “big data.” **O'Toole** mentioned bioinformatics as a key “big data” challenge, where many agencies have a role but DHS might be the lead. S&T is interested in rapid diagnostics and is working with DoD in this area, she said. Discussion continued among **O'Toole**, **Kamen**, **Benda**, and **Bellovin** about randomization, visualization, and other “big data” strategies, and focused on the need to protect privacy while maintaining situational awareness and readiness. **Benda** emphasized the need to ensure both security and anonymity. **Lister** commented on the need to prove effectiveness and to transition solutions. The committee's discussion concluded with an emphasis on industry involvement. **Kamen** mentioned that industry leaders like Google could help S&T in this area.

3. ACCELERATING INNOVATION THROUGH SYSTEMS ANALYSIS

Gerstein briefed the committee members on the systems that S&T uses to engage partners in systems analysis and operational requirements generation. He highlighted the role of the Science and Technology Operational Research Enhancement (STORE) project, the DHS Apex teams, and the S&T Resource Allocation Strategy (STRAS), all of which conduct timely and effective coordination with stakeholders. He described the success of partnerships with the U.S. Secret Service (USSS) and CBP. **Lister** asked how long a typical Apex project lasts, and **Benda** replied that it varies depending on the project. **O'Toole** explained that it is an evolving process of systems analysis and engagement. **Carrano** stressed the importance of feedback and coordination and **O'Toole** agreed, adding that this area is an example of the challenges that operationally-focused Components face when trying to articulate their requirements. **Durham** briefed the committee on systems engineering efforts currently underway with CBP regarding surveillance and response capabilities in the Rio Grande Valley; the following discussion focused on the role of stakeholder engagements, field experimentation, and transition. **Benda** discussed S&T's efforts in the area of agricultural screening tools, and how systems engineering in this area could be used to increase detection and response time for zoonotic diseases, which he said would have a dramatic effect on public health and efficiency of operations. **Carrano** supported this notion, highlighting the massive scale and thin profit margins of many commercial food producers. **Bellovin** observed that any HSSTAC efforts involving systems engineering would also benefit from studying the failures or shortcomings of prior projects. **O'Toole** agreed, while clarifying that in many cases, S&T – and DHS at large – would face criticism for the failures of other organizations or projects in which they were not involved. Discussion continued among **Benda, Kamen, Levis,** and **O'Toole** regarding lessons learned. **Kamen** commented that industry and government could work together in this area; for example, utility companies would be interested because of their concerns about loss of service. He offered to help make connections with industry. **Levis** mentioned the need to show value and market success in a way that is easily understood; for example, using visualization. The discussion ended with a consensus that the need to demonstrate ROI for S&T efforts is critical to long-term success.

4. LEVERAGING INDUSTRY FOR IMPACT

Gerstein opened the discussion by describing various tools S&T uses to guide transition and commercialization, and noted that S&T focuses heavily on tech foraging and learning from industry models and experience. **Benda** commented that HSARPA focuses on building systems that could be leveraged across multiple operational requirements, and highlighted the importance of ensuring that projects stay relevant to customer needs. **Carley** added that crowd-sourcing through university partners could be useful. **Levis** concurred, and emphasized the importance of shaping how partners and consumers consider the implementation of tools at a practical, legal, and cultural level. **Lister** suggested teaming with insurance companies. Discussion continued among **Lister, Carrano, Benda,** and **Bellovin** regarding past examples of disruptive technologies and ways they have been incorporated into society. Smoke detectors were considered a good example, and the committee discussed the evolution of their design, standardization, and normalization. **Carrano** emphasized the cost-benefit analysis and the need to articulate incentives on all ends of the spectrum. **Lister** suggested that pathways to industry be offered as a form of insurance that could evolve into statutes over time. **Benda** mentioned the

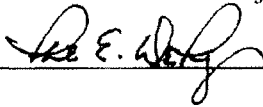
SAFETY Act or SECURE program as a way to cap liability. **Bellovin** responded that the lack of actuarial data can be a problem, especially in cyberspace.

5. **PUBLIC COMMENT:** **Hanson** invited public comment on the above topics. None was offered.

6. DISCUSSION OF NEXT STEPS

HSSTAC Chairman Phil Depoy briefly described the Committee's history and framework and then led the members in a discussion about next steps. **Hanson** offered the use of the Homeland Security Information Network (HSIN) as an option for virtual collaboration and coordination. Several members concurred that a virtual option is a good way to manage scheduling difficulties. **Depoy** solicited member input regarding focus areas and possible subcommittees. **Levis** noted that systems engineering is a likely area for study. **Depoy** agreed, adding that partnering with industry is also key. **Benda** mentioned that input about new starts might be useful, although there is no FY13 budget for them yet. **O'Toole** mentioned that HSSTAC might be able to help identify subject matter experts (SMEs) for new starts. **Kamen** suggested connecting with specific industry SMEs and leveraging them to build prototype solutions. He observed that S&T seems to be well-linked to end users, but lacks good partners "in the middle." **Casani** wondered if HSSTAC should focus more on strategy or more on specific issues. **O'Toole** responded that she would prefer to leverage HSSTAC expertise on specific issues, such as how to teach systems engineering to DHS Components. **Carley** suggested a subgroup to focus on a more unified perspective, perhaps the cyber environment combined with big data and social media, to help define the key issues and who owns which space. **Gerstein** responded that big data in the cyber-environment is a key area but a broad one. **Carrano, Benda, O'Toole, Bellovin, Gerstein, Carley, Lister, and Levis** discussed various areas of potential focus such as biological diagnostics, cyber security, systems analysis and engineering, and networking with interagency leaders. **Carrano** recommended considering a new model for bio-recognition architecture, to leverage economies of scale and sync with industry. **Bellovin** mentioned the need to better understand data visualization. **Carley** mentioned that DARPA is funding projects on visualization in cyberspace, and **Bellovin** cautioned that any visualization efforts must be pertinent to S&T. **Lister** suggested possible ways to help raise the stature of S&T within DHS. **Carrano** suggested that HSSTAC should help identify a few key problems, help S&T to solve them, and then help to market them. **Kamen** commented that technologists seem to always look for a needle in a haystack, when perhaps the focus should be on making the haystack smaller; this would reduce overall cost while increasing efficiency (for example, in airport security). The discussion concluded with agreement on the importance of identifying achievable areas for success, collaboration with industry, and developing good relationships throughout S&T's stakeholder base. **Depoy** closed the discussion by thanking the members for their time and encouraging continued coordination among committee members and with S&T staff.

7. **ADJOURN:** **Hanson** adjourned the meeting at 3:30 p.m.

Signed:  (HSSTAC Chairman Phil Depoy) Date: 12/5/2012

MEETING ATTENDEES

Members:

Steve Bellovin
John Carrano
Kathleen Carley
Julie Casani
Phil Depoy
Dean Kamen
Alex Levis
Mark Lister
Jack Parow

DHS Briefers and Observers:

Georgia Abraham (briefer)
Paul Benda (briefer)
George Boosalis
Troy Byers (briefer)
Gretchen Cullenberg
Bruce Davidson
Shane Davis
Rolf Dietrich
Deborah Durham (briefer)
Dan Gerstein (briefer)
Bob Griffin (briefer)
Herbie Hancock
Mary Hanson
Jamie Johnson
Susan Law
Melissa Mann
Christina Murata
Tara O'Toole (briefer)
Austin Rackets
Sharla Rausch
Ari Schuler
Mark Schroeder (ICE/HSAAC)
Jim Tuttle
Heidi Whiteree
Dick Williams (briefer)
Randy Zeller

Others:

Ken Rapuano – MITRE Corp., former HSSTAC member (briefer)

Members of Public:

John Barsa - MRI Global (VP for Government Relations)
Megan Ignash - Homeland Security Dialogue Forum (Communications Director)
Andrew Jennings - Lews-Burk Associates LLC
Harry Mayfield - Lews-Burk Associates LLC
David Olive - Catalyst Partners (Founder and Principal)
Dave Weideman - PEMA Inc. (President)
Ted Wood - Parks IP Law (patent attorney)

NOTE: All meeting materials (listed below) are posted at <http://www.dhs.gov/st-hsstac>. No handouts were distributed during the meeting.

Meeting Documents:

- Federal Register meeting notices
- Agenda
- Committee Roster
- Speaker Bios
- Member Bios
- Day 1 briefings
- FACA Overview briefing
- Ethics briefing
- HSSTAC briefing
- Day 2 briefings

Read Ahead Materials:

- Homeland Security Act-S&T Section
- Quadrennial Homeland Security Review (QHSR) Executive Summary
- Testimony by Dr. O'Toole subcommittee of the U.S. House of Representatives Committee on Homeland Security on 17NOV11
- Testimony of Dr. Gerstein a subcommittee of the U.S. House of Representatives Committee on Homeland Security on 19APR12
- DHS S&T Strategic Plan 2011
- DHS S&T Year-in-Review 2011



About DHS

[The Secretary](#)

[Budget & Performance](#)

[Careers](#)

[Contact Us](#)

[DHS Digital Strategy](#)

[Do Business with DHS](#)

[History](#)

[Laws & Regulations](#)

[Mission](#)

Organization

[Advisory Panels & Committees](#)

[Department Components](#)

[Leadership](#)

[Office of the Secretary](#)

[Organizational Chart](#)

Science and Technology Directorate Homeland Security Science and Technology Advisory Committee Members

[DHS Press Release Announcing New Members, PDF \(2 pages - 158 KB\)](#)

HSSTAC MEMBERS 2012

Dr. Steven Bellovin

Steven Bellovin is an expert in cyber security, a researcher on computer networking and security, and a professor of computer science at Columbia University. He is currently on leave from Columbia and is serving as Chief Technologist of the Federal Trade Commission. As a former member of HSSTAC and vice chair of its cyber security subcommittee, he co-authored a report advising DHS S&T on how to clarify its cyber security role within DHS.

Dr. Kathleen Carley

Kathleen Carley is a Professor of Computation, Organization and Society in the Institute for Software Research at Carnegie Mellon University. Her research combines cognitive science, sociology, and computer science to address complex social and organizational problems. She established Dynamic Network Analysis (DNA) and has developed tools for analyzing large-scale dynamic networks and various multi-agent simulation systems. Her group has developed tools for text-mining semantic networks, simulating epidemiological models, and simulating covert networks.

Dr. John Carrano

John Carrano is President of Carrano Consulting and the former Vice President for R&D for the Luminex Corporation. A former program manager at DARPA, he is familiar with chemical threats and chemical sensing in both national defense and national security contexts. For the past 10 years, he has focused on clinical diagnostics for infectious diseases and biological agent detection, including the research, development and manufacturing of medical *in vitro* diagnostics products with FDA clearance.

Dr. Julie Casani

Julie Casani directs the Office of Public Health Preparedness and Response in the North Carolina Division of Public Health. As preparedness director of the Maryland Department of Health and Mental Hygiene (1999-2006) she led response to the anthrax events of 2001 and implemented health surveillance systems for bioterrorism. As a former member of HSSTAC, she co-authored a report advising DHS S&T on how best to prepare for bioterrorism threats.

Dr. Phil DePoy

Phil DePoy was the founding director of the Institute of Systems Engineering at the Naval Post Graduate School (NPS) and former president of the National Opinion Research Center at the University of Chicago and of the Center for Naval Analyses (CNA). As a former member and then chairman of HSSTAC, he participated in projects related to biological defense, improvised explosive devices, and cyber defense.

Mr. Dean Kamen

Dean Kamen is an inventor, entrepreneur and advocate for science and technology. He is the CEO of DEKA Research and Development Corporation. He founded an organization called FIRST (For Inspiration and Recognition of Science and Technology), dedicated to motivating young people to understand, use and enjoy science and technology. He was awarded the National Medal of Technology in 2000 and was inducted into the National Inventors Hall of Fame in 2005.

Dr. Alexander Levis

Alex Levis is University Professor Electrical, Computer and systems Engineering and Head of the System Architectures Laboratory at George Mason University and the former Chief Scientist of the U.S. Air Force. The focus of his research has been on organization architecture design and evaluation, adaptive architectures for command and control, adversary modeling for behavioral analysis, and methodologies for architecture comparison and evaluation. As a former member of HSSTAC, he helped advise DHS S&T on how to clarify its cyber security role within DHS.

Mr. Mark Lister

Mark Lister is the President of StratTechs, Inc. a consulting firm specializing in brokering technology within the defense, intelligence, and

homeland security government markets. He served on the Secretary of the Navy Advisory Panel and as Chairman of the Naval Research Advisory Committee. He founded and directed the Rosettex Technology and Ventures Group, a joint venture of Sarnoff Corporation and SRI International. He was appointed Vice-chair of the HSSTAC in November 2012.

Chief John (Jack) Parow

Jack Parow is the President and Chairman of the Board of the International Association of Fire Chiefs (IAFC) and a former fire chief and firefighter. Formerly he served as President of the Fire Chiefs' Association of Massachusetts. He has been certified as a Fire Inspector, a Hazardous Materials Technician, a Fire Training Instructor, and a Domestic Preparedness Instructor for Homeland Security. He is a professor and teaches college courses in fire science and emergency management.

Dr. Yossi Sheffi

Yossi Sheffi is the Elisha Gray II Professor of Engineering Systems at the Massachusetts Institute of Technology (MIT) and is the Director of the MIT Center for Transportation and Logistics and former head of the Engineering Systems Division. He is an expert in systems optimization, risk analysis and supply chain management. His book "The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage" demonstrates how companies should design their operations and supply chains to be able to withstand, major disruptions. He is also an entrepreneur who co-founded five successful companies.

Last Published Date: October 17, 2014

DEPARTMENT OF HOMELAND SECURITY
Office of the Under Secretary for Science & Technology
FY 2008 Report of Closed Meeting of the
Homeland Security Science & Technology Advisory Committee
Under Section 10(d)
Federal Advisory Committee Act

The Homeland Security Science & Technology Advisory Committee (HSSTAC) met in a partially closed session on July 15, 2008 in Arlington, VA. The determination to partially close the meeting was based on the consideration that the briefings and discussions during the meeting would involve classified information sensitive to homeland security. Disclosure of the information discussed could potentially increase the risk to our nation's security due to the identification of vulnerabilities and the potential areas of focus for future research to mitigate our vulnerabilities. All sessions of the meeting were closed to the public pursuant to the provisions of 5 U.S.C. 552b(c) with the exception of the open session on day one.

The objectives of this quarterly meeting were to discuss the last year's Improvised Explosive Device (IED) assessment (IEDs: Coming to America, 29 February 2008); review current committee efforts; and solicit input from attendees on future efforts.

Mr. Norman Polmar, Committee Chairman, welcomed the attendees and explained the HSSTAC, which was established in 2002, met for two years and then went into hibernation for over a year before it was reestablished last July. The committee was asked by the Under Secretary of the Department of Homeland Security (DHS), Directorate of Science & Technology (S&T) to put together an assessment of IED threats in the future. In order to meet this tasking, the committee broke into panels and looked at IEDs coming into the U.S. The methodology for doing this was conducting several interviews and briefings with various organizations, including many British organizations dealing with the IRA and other threats.

The assessment included varying views of what constituted an IED. There are two chains described in the report – the “kill chain,” which describes the steps necessary for the execution of the IED attack; and the “response chain,” used to related counter-IED (C-IED) activities to the terrorist kill chain. The key to effective C-IED measures is to get to the left of the kill chain, or in other words, try to get to people and the sources of the development of the bomb before it is set off.

The IED assessment that the committee finalized included six major findings:

1. The use of IEDs by terrorists within the United States is a real, agile, and complex threat.
2. Countering IEDs in the domestic environment is significantly different from countering them in combat zones based on different operational environments and policies.
3. DHS S&T does not effectively leverage applicable national counter-IED investments.
4. The current DHS S&T IED program is primarily focused on countering the devices and does not have sufficient emphasis on the human component of the IED threat.
5. DHS S&T does not sufficiently incorporate the requirements of diverse local, regional, and state responders in its planning.

6. DHS research and development (R&D) programs do not effectively support social and economic resilience to IED attack and post-attack restoration, although this role for DHS S&T is limited under the enabling legislation.

Each finding was briefly addressed during the committee meeting. For Findings #1 and #2, the threat is unlikely to be eliminated, because most potential terrorists expect to terminate themselves. Their goals are to create a loss of confidence in the US government and to force US isolation and withdrawal. Their targets are symbols, economic, infrastructure, and mass casualties. Furthermore, although there is generally broad leeway in Afghanistan and Iraq for IED counter-measures, in the US there are severe legal and social constraints.

For Finding #3, it was noted that the report was an assessment, so it is very critical of DHS and other federal organizations. The observation for Finding #4 was that most of the effort is in getting the device, so there is a need to continue to push interest and investment further to the left of the actual detonation. Finding #5 noted that S&T needs to better prepare first responders for the long term. Most of the first responders are volunteers so it is difficult for them to devote a lot of time to their jobs as first responders. This is very different from being a full-time federal employee, whose sole job it is to act as a first responder.

Finally, for Finding #6, S&T currently has inadequate R&D programs to support rapid restoration of social and economic activities after an IED attack.

Next, the leaders of the three HSSTAC Panels presented their progress.

Program Assessment Panel

Dr. Lawrence Papay of the Program Assessment panel presented his panel's objective and tasking to review, assess, and make recommendations with regard to relevance and completeness to the Under Secretary for S&T. Seven specific taskings were developed for the panel: 1) review the scope of S&T's mission; 2) evaluate strategic planning and operations; 3) get an understanding the S&T program; 4) review financial performance; 5) assess relationships with other S&T organizations; 6) review S&T directorates and how their process is tracked; and 7) provide recommendations on the health and quality of the S&T programs. Since there are several audiences for this panel's pending report, it can serve as a transition between administrations. Congress also requires updates on an annual basis.

In order to complete its taskings, panel members have talked to S&T Division Directors, the Chief Financial Officer, the Homeland Security Institute, and representatives from first responder organizations; they also plan to talk to Congressional staffers. A timeline was made in March 2008, and they have had meetings in April and June. They have been in fact-finding mode until now, and will start talking about where to go next and begin drafting the report in August.

Cyber Threat Response Panel

Dr. Richard Roca is the chair of the Cyber Threat Response panel. The panel's concern is the fact that the cyber domain is dynamic and evolving, so a constant evolution in the

measures taken to protect and defend it is necessary. The question becomes how technology informs procurement for various mechanisms. Multi-level security is involved, and the focus is on the reconstitution, remediation, and response to potential threats.

Cyber protection was compared to the anti-submarine program in the Navy, and the question was asked: Is there an analogous application (physics-driven) that can be used in the cyber world? There are several complications to government adapting to technological changes. Moore's law states that the government takes 18-24 months to adjust and adopt a new technology. However, by that point, the technology is already obsolete and more technologically advanced adversaries have already adjusted and adapted to a faster and more dangerous form of technology. The final panel report on cyber security will outline the issues and discuss what long-term investigations should focus on.

ChemBio Panel

The third panel, the ChemBio panel, is chaired by Dr. David Franz. Dr. Franz presented the timeline for the ChemBio Report, giving August 1st as the deadline to have the draft completed. Before 1997, all ChemBio defense work was done in DoD. There was a \$37 million budget until 9/11; afterwards, this number jumped into the billions. The terms of reference for this committee were to understand the form and function of S&T but focus on the seams between assets and stakeholders within and outside of DHS. Dr. Franz then presented the mission, 5-year deliverables, and recommendations that the report will include.

The panel briefings concluded this meeting. The next meeting of the HSSTAC will be on October 20-22, 2008 in Norfolk, VA.



Ervin Kapos
Designated Federal Officer

Summary of Meeting – Public Session

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security Science and Technology Advisory Committee (HSSTAC)

At

**William F. Bolger Center for
Leadership Development
Potomac, Maryland**

February 26, 2004

Meeting Summary:

This summary describes the discussions of the inaugural meeting of the Homeland Security Science and Technology Advisory Committee (HSSTAC). The meeting was held from 11:00 AM – 2:00 PM on Thursday, February 26, 2004 at the William F. Bolger Center for Leadership Development in Potomac, Maryland.

The HSSTAC met for the purposes of: (1) welcoming and introducing members of the committee; (2) receiving briefings on the mission and organization of the Department; (3) receiving briefings on the mission and approaches of the Science and Technology Directorate; (4) holding roundtable discussions with the committee members; (5) discussing the role of the committee in advising the Department; (6) receiving briefings on detailed historical background, organization, programs, accomplishments and plans of the Science and technology Directorate; (7) receiving briefings on activities on activities and accomplishments of the Office of Research and Development, the Homeland Security Advanced Projects Research Agency, the Office of Systems Engineering and Development, and the Office of Weapons of Mass Destruction Operations and Incident Management.

Participants:

Committee Members in Attendance:

Larry D. Welch, Chair
Ronald M. Atlas
Russell W. Bessette
Lillian C. Borrone
Bran Ferren
Baruch Fischhoff
Alice P. Gast
William Happer
Anthony P. Ibarra
Ted G. Kamatchus

Ernest Mitchell
Lawrence Papay
Richard T. Roca
Kenneth I. Shine
Reginald I. Vachon
Vincent Vitto

U.S. Department of Homeland Security Representatives in Attendance:

Charles E. McQueary, Under Secretary, Science and Technology
Penrose C. Albright, Assistant Secretary, Science and Technology
Victor J. Tambone, Chief of Staff, Science and Technology
Ronald D. Taylor, Executive Director, Homeland Security Science and Technology
Advisory Committee
Georgia Abraham, Acting Committee Management Officer, Office of the Executive
Secretariat
John Mitnick, Associate General Counsel, Science and Technology
Nicole Marcson, Office of the General Counsel, Science and Technology
Mary Karen Walker, Office of Research and Development, Science and Technology
Craig Wilson, Office of Studies and Analysis, Science and Technology

Members of the Public in Attendance:

Approximately 20 members of the public attended the meeting.

HSSTAC Meeting Called to Order

DR. TAYLOR: My name is Ron Taylor. I'm Executive Director for the Homeland Security Science and Technology Advisory Committee. General Welch, Under Secretary McQueary, Mr. Tambone, distinguished members of the Homeland Security Science and Technology Advisory Committee, members of the public, I'd like to welcome you to the very first meeting of the committee. This is a special moment for all of us. And I'm sure this is -- with the first anniversary celebrations that are taking place this week for the Department of Homeland Security -- one of many special moments during this week that will appropriately mark a unique step in the history of this country. With that, I would like to turn this meeting over to the Chairman, General Welch.

GENERAL WELCH: Thank you, Ron. I'll add my welcome to members of the committee and those who serve in the Department of Homeland Security, and those members of the public that might be here.

As Ron has noted, this is the inaugural meeting of the Homeland Security Science and Technology Advisory Committee. I'm Larry Welch, Chairman of the committee. We are getting ourselves organized. A reminder to all of us that this committee was established to provide independent scientific and technical planning advice to Dr. McQueary on areas within his responsibility, which are extensive and very important to the country, and therefore, important to everyone in this room. I will not spend any time on the responsibilities he carries, since we will hear from him a bit later.

Let me say, though, that this committee will focus intensely on providing useful advice to Dr. McQueary. Our membership has been selected to insure that the group is made up of distinguished and accomplished people who bring the expertise in science, engineering, medical research, industry, academe, and government that should make it possible for us to provide useful advice. And that's how we will grade ourselves.

I think it will facilitate our work if we begin this meeting by mutually understanding the expertise and the experience and the perspective that each of us brings. To that end, I would like for each to take three or four minutes to provide that introduction on who you are, what your interests are, and what your qualifications are that might relate to the work of this committee. I will start, and then I'll move to Dr. Fischhoff to follow me.

As I said, I'm Larry Welch. I served 40 years in the military, two years in the National Guard and 38 years in the Air Force as a fighter pilot, systems analyst, planner, programmer, and operational unit commander. I completed my Air Force service as Chief of Staff and moved on to become the president and the CEO of the Institute for Defense Analyses for 13 years. My particular focus for a number of years has been enabling more effective operations through technical, operational, and policy innovation. I hope that same focus will be appropriate to Homeland Security, and I'm sure it will be.

DR. FISCHHOFF: My name is Baruch Fischhoff. I'm a cognitive psychologist and decision scientist at Carnegie Mellon University. I'm in two interdisciplinary departments. One is called Engineering and Public Policy. The second is called Social and Decision Sciences.

In the first, we try to integrate analyses involving social, natural, and engineering sciences. In the other, we try to do more basic research that involves the interface of psychology, economics, management, science, and operations research. So we try in both to bridge the disciplines and to bridge basic and applied research. My specialty is decision-making having to do with risks. I serve on a comparable body, the Environmental Protection Agency Scientific Advisory Board, and President-elect of the Society for Risk Analysis.

I think there are three aspects of human behavior that I would hope that I can contribute to this committee's activities. One is in the area of risk communication. That is, helping the public to understand what it's up against and what it is that we're trying to do on its behalf. And conversely, to hear from the public what are the issues that it wants to have addressed, and what are the kind of policies that the public believes are necessary to facilitate better risk communication.

The second area where I see behavior as being important is ensuring that our plans are behaviorally realistic. That is, we have expectations about how the public will respond to various actions, our own or of our enemies, in times of peace, in times of crisis. And it's important that we take best advantage of the best available social and behavioral science

to make certain that we have plans that work as they're intended, and are realistic, so we know the limits of our own understanding.

And the third area is that in the making of plans, human activity requires the exercise of intellect, the integration of data, and human judgment. And that's another area that people like me work on. So we would like the best available plans and analyses that we can get from our technical experts. But for those of us who have operational responsibilities and need to rely on those plans, we need to know just how good they are. We want to know whether they've done a terrific job of analyzing the stuff that's easy, but have left out a lot of stuff that's difficult.

MR. FERREN: My name is Bran Ferren. I'm currently Chief Creative Officer and Co-Chairman of a company called Applied Minds. We're interested in the impacts of technology on the world, and how to make the world a better place.

Prior to that, I was President of Research and Development and Creative Technology for the Walt Disney Company, where again, the focus was what is the future of the entertainment industry? How does technology pertain to that?

I come from a mixed background -- equal in art and design and science and engineering. I've always found both fascinating. I never quite decided why one should have to pick one or the other, and so you end up not knowing what you do for a living.

My interests are in design and all aspects of it, whether that's design of systems and system engineering, whether it's design of components or products, whether it's design of organizations, whether it's design of environments that make people work better and more effectively at high-performance jobs. All aspects of design interest me.

I find that the impact of technology on people's lives and how technologies can be used and focused to better mankind and civilization to be something of particular interest. And whether that's on an organizational basis within government or outside of government, we are living in a world where the only thing that is constant is that nothing is constant, and that change is around us. It's not just that change is accelerating, but the rate of change is accelerating. And the implications of how one deals with this to effectively predict and shape the future of our nation is something of great personal interest as well as what our company does for folks like General Motors and Northrop Grumman and a bunch of government agencies.

I spend my spare time -- and I use that guardedly -- on a number of government advisory boards in the areas of technology, intelligence, and again, basically, innovation of organizations and systems.

MR. IBARRA: My name is Tony Ibarra. I am CEO and founder of Digatron, Incorporated. We're based in Denver, Colorado, and have been in business for 23 years. We offer electronic surveillance systems integration, design, distribution, and manufacture digital video recorders.

I believe what I have to bring to this distinguished committee is that we as a small business were probably one of the first that brought digital video recording to the government sector. Some of our client base includes the U.S. Capitol; the U.S. Department of Justice; Federal Bureau of Prisons; U.S. Department of State, where we have deployed our digital video recorders throughout the country, where they can view all the cameras throughout the country in D.C. And we have recently contracted with Department of Homeland Security to secure the northern and southern borders of the United States.

I'd like to read a statement that Under Secretary McQueary made before the U.S. House of Representatives not so long ago. "The most important mission for the Science and Technology Directorate is to develop and deploy cutting-edge technologies and new capabilities, so that the dedicated men and women who serve to protect and secure our homeland perform their jobs more effectively and efficiently."

I believe from a small business perspective, because we have been able to deploy technology on a rather quick basis, that we can continue to do that from the small business sector.

I'm also extremely proud to be part of Homeland Security's Science and Technology Committee, and look forward in determining ways that we can secure our homeland.

SHERIFF KAMATCHUS: My name is Ted Kamatchus. I'm the sheriff of Marshall County, Iowa. I'm just beginning my seventeenth year as sheriff. I have 28 years in law enforcement beginning at the small-town levels in Minnesota, and working my way up until being appointed sheriff 16 years ago.

I'm 3rd vice president of the National Sheriffs' Association. I have been very active in that association since 1993. I have chaired several committees for them; a couple on science and technology. I'm also a commissioner on the Board of Commissioners for the Commission on Accreditation for Law Enforcement Agencies, the internationally-known and acclaimed accrediting body for law enforcement throughout the country and across the world.

I've been on various law enforcement boards over the years, from president of the Iowa State Sheriffs and Deputies, and reserves in several areas.

I think what I really bring to this committee is the perspective of somebody who's actually on the road, actually doing things. Being from a small rural area, being very active, we deal with many things that come out of Washington, D.C., and many things that come out of the state capital of Iowa. And oftentimes, some of the best-laid plans, if you will, don't fit the road, and they still make sense.

And I hope that I can give you some input and listen to some of the things, so we can take those things and put them to good use so that we can have a positive effect when we're all said and done here. It's going to be a great learning experience for me.

I've had an opportunity to participate in other technological areas dealing with interoperability and communication and data exchange. And I hope that I can give some input based on those other experiences, my experience on the road, to help this committee and do a good job for the country. I'm looking forward it. Thank you.

DR. ATLAS: My name is Ronald Atlas. I'm Graduate Dean at the University of Louisville, where I'm also the co-director for the Center for the Deterrence of Biowarfare and Bioterrorism, the immediate past president of the American Society for Microbiology, and also for many years headed their task force on bio-weapons.

I have a background in microbiology, particularly in environmental microbiology, and detection methods for pathogens in the environment. We also now work in training physicians to recognize bio-threat diseases, and in developing public health communication systems. So my background and expertise is in the deterrence of bioterrorism.

DR. HAPPER: I'm Will Happer. I'm a physicist by vocation. I specialize in nuclear physics, lasers, magnetic resonance, both basic and applied. I've worked many years with the Federal Government on applications of science and defense.

I was a member of the National Academies committee put together after September 11 that issued the report titled *Making the Nation Safer*. I chaired the sub-panel on counters to nuclear and radiological weapons. I recently returned from Moscow a month or so ago looking at how well they're safeguarding their highly-enriched uranium and plutonium. So this is something that I have a very deep interest in, and I hope I can contribute in that way to this committee.

DR. SHINE: I'm a cardiologist and physiologist by training. I started out doing basic laboratory work, but got very interested in policy at an early stage when with another colleague, I was the leader of an effort to get a 911 number in Los Angeles County, where there are 84 jurisdictions. So I know a little bit about the difficulty of translating better health into public policy.

After serving as Dean at the UCLA School of Medicine, I went to the Institute of Medicine in 1992 and was President there for 10-1/2 years, where we did a number of studies with regard to metropolitan response before 9/11. And then immediately after 9/11, with my colleagues, we convened the committee that produced *Making the Nation Safer*. You can see by some of my colleagues here that we identified some very high-quality players for that activity.

For the last five years, I was a member of the Gilmore Commission, that was responsible for looking at issues of domestic terrorism. And I'm very interested in the problem of

technology transfer for first responders; how we find the right technologies to help them, how we educate them and ourselves as to the best ways to use that technology. And first responders, from my perspective, include the full range from police, fire, and medical people, to the media.

When I finished my term at the IOM, I established the RAND Center for Domestic and International Health Security where we developed strategies for evaluating public health preparedness at the local level using a variety of techniques.

I chair the Scientific Advisory Committee for the Food and Drug Administration and there I'm very interested in issues related to food safety and the use of technology to improve the way in which both food and medications are available. I'm very interested in vaccine policy, vaccine development, and patent policy.

I currently serve as Executive Vice Chancellor for the University of Texas, which, as you know, has just been awarded one of the two BL4 bio-containment laboratories. The University of Texas also has major activities in areas related to the biology of terrorism.

MR. TAMBONE: My name is Vic Tambone. I'm the Chief of Staff for Dr. McQueary. I've served 24 years in the Air Force as a pilot. I've served in staff and command positions. After I retired, I did some private sector business. And since the 24th of March, I was Dr. McQueary's Chief of Staff. I'm here to help Dr. McQueary, General Welch, and all of you to make the trains run on time, do whatever I can to make this a successful committee.

GENERAL WELCH: We will hear from Dr. McQueary in some detail later.

MR. VITTO: Hi, I'm Vince Vitto. I spent 39 years in the not-for-profit research and development sector, 32 of those years at MIT's Lincoln Laboratory, which is a federally-funded research and development center, and the last seven years as President of the Charles Stark Draper Laboratory, which is an independent not-for-profit, originally part of MIT, sponsored by MIT in 1973. We've been independent but not-for-profit over the last 20-some-odd years.

My areas of interest and expertise have been in space systems, dominantly space surveillance and communications, while at Lincoln Laboratory. Typically, most funding, and most work have been with the Department of Defense. Draper Laboratory is more involved in guidance, navigation and control, issues associated with ballistic missiles, tactical systems, and work for NASA.

I've been involved in government advisory committees for the past 25 years, dominantly for the Department of Defense, but also for the National Research Council, the National Academies, and some for NASA. I'm currently Vice-Chairman of the Defense Science Board. I'm Chairman of the NRC Naval Studies Board, and was a participant with Will Happer on the National Academies study that produced *Making the Nation Safer*.

On that study, I chaired the Systems Engineering Panel, and I was also asked to develop the section of the report that dealt with the cross-cutting technologies that came out of the study. I view myself as a systems engineer, and the systems engineering infrastructure protection aspects of Homeland Security is where I have interest.

DR. GAST: My name is Alice Gast. I'm a chemical engineer. I work in physical chemistry of surfaces and so-called complex fluids, which are just about anything that you'd like -- small particles, proteins, polymers.

I taught for 16 years at Stanford University, where I was involved with the Stanford Synchrotron Radiation Laboratory, and more recently involved in their Bio-X initiative to integrate science and engineering with medicine.

My research has focused on understanding the basic and fundamental processes in these complex fluid systems. More recently, it's evolved into so-called microfluidic devices, and more biophysical problems involving membranes and proteins.

A little over two years ago, I moved to MIT and assumed responsibilities as Vice President for Research. And in that role, I feel that my job is really to be the champion of interdisciplinarity, and MIT is a wonderful place to have that job. There are many opportunities where research cuts across disciplinary boundaries and brings together individuals who had not worked together previously for the purpose of producing new and exciting innovations. I think that's one area that I hope to contribute, both the bringing together of different people and topics from different backgrounds, as well as integration of research and education, which I think are so fundamentally important.

I also have been involved with some of the NRC counterterrorism work. I assumed the co-leadership of the Board on Chemical Sciences and Technology in the NRC in October of 2001, and I spent quite a bit of time looking at issues related to chemical terrorism and potential threats based on either our chemical industries or chemicals themselves. And so I've thought quite a bit about those issues, and hope to contribute in that way.

DR. PAPAY: I'm Larry Papay. My career has spanned from training and education to nuclear engineering. And then after doing some post-doctoral work in Europe on nuclear technology, I joined Southern California Edison, a utility, with the express purpose of starting up a research and development function at an electric utility, which was rather novel and unique in 1970.

In my career there, at one time or another, I had responsibility, as I like to say, for everybody but the lawyers and the accountants. Those experiences gave me access to knowledge of how to run an electric power system, an interconnected grid in the western part of the United States -- that's the Western Systems Coordinating Council -- power pools. And actually, Southern California Edison at that point in time had the fifth largest telephone system in the state because of its need to communicate internally.

After leaving Southern California Edison, I joined the Bechtel Corporation, heading up their technology and research organization. This gave me not only additional insight from an energy and environmental point of view, but exposure to and involvement in a more or less civil infrastructure because of the heavy dealings that a company like Bechtel has in those areas.

Four years ago, I joined SAIC Corporation, headquartered in La Jolla. SAIC is a very large government contractor, which is really a systems integrator, as well as being involved in a variety of technologies.

My position on this committee is for expertise in critical infrastructure other than information technology. I think it's quite evident that the more evolved a civilization is, if I can call it that -- or a society is -- the more fragile its infrastructure is, because it's more vulnerable, it's more complex. And if it's more complex, by necessity, it's more fragile.

If you compare the infrastructure here to what we commonly call Third World countries, critical infrastructure here is on an entirely different level, and the threats are entirely different in many respects than they are in other countries. This was brought to my attention most recently by taking part in a joint U.S./India symposium of how science and technology can counter terrorism. Their level and their concerns on terrorism are entirely different than ours. I'm not sure whether we're better off for that or not. And so I look forward to participating in the work of this committee, particularly as it might address issues such as these.

And just as a footnote, I also contributed to the National Academy report *Making the Nation Safer* in what originally was going to be one chapter and ended up being two; one on energy and one on cities and fixed infrastructure.

DR. ROCA: My name is Rich Roca. I am the Director of the Johns Hopkins University Applied Physics Laboratory, and I've been there since January of 2000. APL is a division of Johns Hopkins, and is a university-affiliated research center, in DOD jargon.

We focus in two broad areas. One is complex combat systems largely for the Navy, whether it be undersea surface or in the air, and the other is space science and technology, both for DOD and for NASA. The work originated because of the need for satellite technology in the '50s and '60s in order to advance at that time the Navy's agenda with precision navigation. And as people put more technology and complicated systems in the space, they discovered they knew less and less about space, and required the space science to go along with it.

Prior to coming to APL, I was at Bell Laboratories for over 30 years, or whatever Bell Laboratories was called as the Bell System morphed into its various forms. I left there eventually responsible for all the Internet services of AT&T from the R&D perspective.

I've been involved in large-scale communication systems -- if you will, the telephony analog to the electrical grid system that Larry just described -- concerned with how you design them, how you plan them, how you get the customers' expectations met, how you keep them going on sunny days and how you keep them going on rainy days. So I have one way or the other been involved throughout my career in the systems engineering and operations of fairly large-scale systems that had to withstand both intentional and unintentional disruptions, and how you plan for that.

DR. BESSETTE: My name is Russell Bessette. I am presently the Executive Director of the New York State Office of Science, Technology, and Academic Research. And in that capacity, I report directly to the governor, Governor George Pataki. Our agency was created in 1999, and in the past four years, has been an agency that has invested over one billion dollars in New York State universities in science and technology.

This has been a very interesting and challenging position that I've had for the past several years in being able to work with the universities and private enterprises in collaboration and identifying cutting areas of research, and investing in that research to create jobs and have economic impact within the state.

In the year 2002, the agency undertook a program, because of the events of 2001, that was focused in the areas of science and technology as applied to terrorism and issues surrounding security. And we have had a number of programs that have ranged from sensor detections of pollutants to water supplies to air contamination, and ranging from bioinformatics to nanotechnology.

In my prior life, I was a physician and surgeon. I trained as a general surgeon and as a head and neck reconstructive surgeon, and practiced for 23 years. I served as clinical professor in the State University of Medicine at Buffalo, as well as Department Chairman. I've served on President Bush's Transition Team as an advisor to the identification of new areas of expansion for the National Institute of Health, and have served as a private physician and six years in chairing the New York State Public Health Council.

CHIEF MITCHELL: My name is Ernie Mitchell. I'm the President of the International Association of Fire Chiefs, and the Fire Chief and Assistant Director of Disaster Preparedness in the City of Pasadena, California.

First, I want to thank Dr. McQueary and this Administration for the insight and the vision to include the first responder community in this effort to enhance and improve our ability to respond to events of terrorism and prevention.

As President of the International Association of Fire Chiefs, we have over 12,000 members across the country, as well as chiefs from foreign countries. Our primary purpose is to service and support those leaders of the fire service. So I look at this as an opportunity to open up an exchange with that community as well.

On a more personal note, I guess, I've been interested in technology all my life. I was an engineering student until I got sidetracked by the fire service. I'm most interested, both personally and professionally, in the opportunity for technology transfer, so we might better protect the first responders and our communities. And so I do see this as an outstanding opportunity for fire service and first responder involvement, and just looking forward to the possibilities that are before us.

GENERAL WELCH: I thank everyone for those very focused and concise descriptions of your experience and interest. It bodes well for the committee that we did that in half the allocated time, which says that you all are indeed focused and concise. And we hope that that will characterize our future discussions.

But in any case, as you noted from the e-mails you received, that we will be forming initially four subcommittees in order to actually do the work of the committee in a more productive environment than having 20 of us sit around a table. And we will form some recommendations based on your expressed interest and your experiences. We will talk more about that later. But it seems very clear that the range of experience and interests will very well match the range of challenges that Dr. McQueary has to deal with.

We are a bit early for lunch so I would ask Dr. McQueary to start and we can break for lunch at a convenient spot.

DR. MCQUEARY: First of all, let me thank each of you for agreeing to be a part of this activity. I can't tell you how important the role that you have agreed to be a part of is to not only the Science and Technology Directorate, but also to the Department.

I guess one of the things that you might ask yourself, how did we end up with the collection of you? As, of course, part of the legislation that created the Department of Homeland Security, we are required to have a Science and Technology Advisory Committee. And in addition to that, the Congress helped us out by being pretty specific about the number -- 20 people -- and category of backgrounds and capabilities that we should have on the committee.

When I first read the statute over a year ago, I thought, "Well, this is a strange collection of talents." After I got into the job, it became readily apparent that there was a great deal of foresight, and I thought Chief Mitchell summarized it very well as to why it's really important.

The Science and Technology organization exists as a service organization to the operational units that make up the Department of Homeland Security. Without the operational units, there would be no need for us to exist, because there's plenty of good science that goes on out in private industry, universities, as well as in the government too, and the various labs that are there.

So it's one of those areas where we exist in what I call a customer/supplier relationship, and that the Science and Technology Directorate has the responsibility to provide the

very best sites in technology, either directly or in an informational sense, to those operational units.

And the operational units, if you are not intimately familiar with how the Department is organized, are the Borders and Transportation Security Organization, Emergency Preparedness Response, Information Analysis and Infrastructure Protection, Coast Guard, and Secret Service being the major areas that we have responsibility for within the department.

Within that, the technologies that we talk about that we have to deal with are chemical, biological, radiological, nuclear, high explosives, cyber, and standards. And so when you take all of that together, for me, who is trained as a mechanical engineer, that's quite a wide range of scientific areas of responsibility that the Department has, and it obviously represents the kind of threats that this country faces from those who would do us harm.

So with that said, I think it becomes clear why the range of capabilities that we have represented by you on this committee is so important. While we may find interesting science to do, we must focus on the needs of the first responders. We must find ways to take technology to the field so that people who may not be trained as engineers -- very likely will not be -- nor have scientifically-based backgrounds can use the equipment, have high confidence in it, and know that it is doing things in order to make it easier for them to do the jobs that they have to do. Because in reality, whenever an event happens in this country again -- and it will -- it's the people that are the first responders that need to be given the best tools available in order to be able to do the jobs that they have to do.

So it is very important to me -- and my background would certainly drive in this direction -- it's very important to me that this organization deliver things. We are not in this business for scientific curiosity or looking to further science, necessarily, although that outcome could very well be a byproduct of what we do. The real important responsibility we have is to engage in those scientific areas that can result and will result in providing capability to first responders so that they can do the jobs that this country depends so strongly upon for its security and that of its people.

So with that background, that's the first half of what I would say. I do have some prepared remarks that I thought I would go over some parts of this to give you more of a sense of not only what the Science and Technology organization is all about. But I don't want to talk too long. Because what I would really rather do is have a chance for you to ask questions that might be on your mind. Because as we get started, we're all coming at this from different backgrounds, different venues, different areas of experience and knowledge about what we have to do.

So I think it's really important that we get on common footing in order to be able to do that. And I know General Welch would do that. And I want to publicly say thanks to you, General, for being willing to chair this very important group, and I look forward to working closely with you, as well as the other members of the organization.

Within the department, within Science and Technology, we get lots of people who have inputs in what we do. In fact, the Congress, as you know, has a lot of interest in what our responsibilities are. I spent two hours yesterday with Congressman Mac Thornberry and his Committee on Cyber Security, Science, and Research and Development, and there's a lot of interest -- a lot of supportive interest, I might add, in what we're doing within the organization. And so we get a lot of inputs, a lot of help. But ultimately, we have to have a plan of action and of execution as to what we're going to do.

I guess a question for the members of the committee. How many of you knew some other person in this group before you showed up?

(Show of hands.)

DR. MCQUEARY: All right. So we have more than half who knew someone else that's in the group. How many of you only knew one other?

(Show of hands.)

DR. MCQUEARY: All right. It's interesting. So we're going to get a chance to know one another and know what our capabilities are. So I think that's good for us.

GENERAL WELCH: A question for you, although if it's in your remarks, we can wait. The breadth of responsibilities that are called S&T in the Department of Homeland Security is significantly different than what's called S&T in other departments. It would be useful for us to be sure that we understand your view of that breadth.

DR. MCQUEARY: I'll give you sort of a top-level view of that in my four immediate reports, and I'll comment upon organizational structure as I get into this. But the four people who report to me are each going to come and give you rather extensive discussions about what they do as a part of that. And we'll start later with Dr. Parney Albright, assuming he was able to get out of a wet California on the red-eye last night.

I started to talk a moment ago about how we chose each of you. We actually looked for and received nominations and recommendations from many sources -- individual and organizational. As one example, and as called for in the statute, we used the National Academies. We then put you and all the nominees into categories associated with the kinds of expertise we needed. And so each of you were slotted into one or more areas where you might be able to communicate.

We then went through -- looked in detail at the biographies that we had on each of you. Because there's only two of you that I actually knew before I met you, and that was Will Happer and Rich Roca. And Rich and I worked together for many years at AT&T. But the rest of you, I don't believe we had met previously.

We went through putting you in categories of where we thought you could best serve, based upon your biography and information that we had. We then went through an

individual selection, made a recommendation to the White House as to which individuals we wanted to choose. And I think with the exception of one individual out of the recommendations that we made, we got approval for what we wanted to do. So you are the first team, and I want you to know that.

Let me talk a little bit about what the mission for the Department of Homeland Security is, and we've been working on the details of that. But fundamentally, the mission is that we will lead the unified national effort to secure America, and we will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. And we will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce. That is the large over-arching reason why this department exists.

And the strategic goals for the department are centered on anticipating and responding effectively to terrorist threats in the scientific areas I talked about earlier, and taking the steps to reduce loss of life, restore services, and rebuild should an attack occur.

And, of course, we all know of the attack in New York. We also can look at how quickly the country responded in order to clean up that terrible tragedy and to move onward with what we're doing there. And I think that's a mark of what this country is all about. And, of course, in doing all of this, one of the great challenges is to make sure that we do have awareness.

I'm particularly interested in the comments that were made earlier, and I apologize for not getting all the discussions earlier. I think the point you made about communication with people and making them aware is really an important part of what we do. And, in fact, you'll see in this calendar year more activity throughout the department of trying to make sure that we do have better communication. Because an informed public will go a long way towards helping decide what needs to be done.

Because if we have an event, you can't sit and say, "Well, what does Washington now want us to do?" People have to have in their minds, just as they do now when we have catastrophic events in this country, we used to lose a lot more people in hurricanes and tornadoes than we lose now, because -- and I believe that, and I think the evidence bears this out, that the reason we don't have as many people killed is because we've done a better job of educating the American public as to what needs to be done in those times of crisis, and we've got to do a similar thing with the public as it deals with terrorism.

Well, on March 1st, the department will be one year old. It's hard to believe we've been at this a year, in one sense. And in another sense, it seems like it's been 10, because there are lots of things that are going on. And we do have a number of activities going on this week to celebrate that.

We have ramped up very rapidly in the department. There were many people who said it was impossible to take 22 agencies, combine them into one operational organization. And while none of us would declare victory, I think we would certainly say that we made

a large amount of progress, very good progress, particularly in the borders area where we have one face at the border, and the people that once represented three different governmental organizations in three different departments now work under one secretary, and I believe are performing better every day in the jobs that they have to do.

We had transferred in to us, obviously, the Coast Guard and Secret Service, two great agencies. If you don't know people that work in those organizations, you're missing a great opportunity to know some fine Americans and people who do first-class work.

Of course, the FEMA organization also existed prior to the formation of the department. And so really, those three things represented a tremendous foundation which the department could build upon to go forward.

And so I think those who said we couldn't make the combination failed to recognize that we had a tremendous foundation and capability to begin that building, and also had a great motivation among the people.

Just to let you know how large this problem is, I'll go through some statistics very quickly.

We have 95,000 miles of shoreline. We have 7500 miles of shared border between Canada and Mexico. We have 621 border points of entry into the United States.

And, on a daily basis: One million people cross those borders. There are 360,000 vehicles that come across the borders. There are 5100 trucks crossing the borders. Twenty-six hundred aircraft come into the country, including international flights. There are 600 vessels that come in to shores every day. We have 10,000 shipping containers.

And so if you go through all of this, it's roughly over a over a million operations a day that the department has an interaction of some sort, and all we have to do is be right 100 percent of the time. And so those of you who are statisticians and know a little bit about it, talking about what kind of error rate you can have, you're dealing in 10 to the minus six and smaller numbers.

So it's a very, very low error rate that we can tolerate. And when you consider that people are involved in these transactions, it's a tremendous responsibility that we have. And I, quite frankly, have not encountered anybody who says, "I don't want to do it, because it's too hard." We've got a lot of committed people that are ready to do what they think we need to do.

On top of that, the adversaries only have to be right once. So we have a tremendous responsibility and many interesting things that we have to do.

I think we all know that it's impossible to guard against all threats. I mean, no matter how hard we might work, we certainly know that there are things that people could do on small and large scales. And one of the things that we have to do and are doing is to

establish good relationships with both the Canadians and the Mexicans in order to be able to do the jobs that we have to with them, because we cannot deal with the border issues as just a U.S. issue. It's a bilateral issue that must be dealt with by both of those, and we've made great strides in that area.

I was fortunate enough last week to be able to go to Mexico City with the Secretary and a delegation to interact with the Mexican Government. Secretary Ridge signed some agreements on relationships with the Mexicans as to how we'll be working with them.

I had a chance to spend a couple of hours with the scientific groups in Mexico to understand a little bit about some of the challenges that they face. And one of the things that became obvious in the discussion is they have a tremendous problem on their southern border of people coming in from Central America.

And, in fact, that's a path, a clear path, where many of the difficulties that we have on our southern border finally manifest themselves. And so we're going to take a small team of people to work with them to see if there are some things that might be done to help them in their southern border area.

There's a choke point where I'm told where only a railroad and one road for traffic, automobile and truck traffic, comes through. In addition to that, it's an area where we may be able to use technology that would not be applicable to our southern or northern borders, because it takes too long. Whereas there, you have a longer period of time, and perhaps there's something that we can do in that area. So it's very important that we have good international relationships.

Also, in addition to those two I mentioned, we've had a number of interactions with the Israelis. And, of course, the Israelis have dealt with the issue of terrorism more than any other country and have made strides. And even today, the Israelis still have been unable to thwart suicide attacks. And that, of course, is not something we've experienced in this country. It would be an easy thing to do and a very difficult thing to protect against.

We've had a small group of scientific people go to Japan to maintain the proper level of interaction. So we're trying to make sure that we have the right level of international activity and connections where it makes sense.

Let's talk just a bit about the mission of the Science and Technology Directorate within the department. We have, really, four areas that we talk about. And I'll just briefly touch upon those, and I'll go to the organizational structure.

We're to partner with the operational end users to identify requirements and develop and field capabilities to counter threats. And I think it's really important to recognize when I say partnership, it truly has to be a partnership, because we need to know end-user requirements. And there's at least two ways that we can get that information.

It may be possible in many cases for the end users to specify what their requirements are. In some cases, it's not possible. They don't understand them well enough. I think in all cases, people can describe the problems they're facing. And in the latter case, I would view it as a responsibility of the Science and Technology Directorate to help turn problems into requirements that can be used to solve those problems, and we take that as a serious part of our responsibility.

We have a multi-pronged approach to engaging the scientific community in this country. It's important that we be engaged with not only those in government, but also in academe, as well as in private industry, to make sure that we're capturing the very best talent that we can for the kinds of things that we must do.

At least two or three of you touched upon something that is probably the foundation of my whole being in terms of the job that we have to do, and that is systems engineering. I truly believe that the basis for what we do in this department has to have a firm systems base for going forward.

I think it's important that we be able to characterize this "Homeland Security system" that we have at some level. It is important that we be able to characterize where we need to get to. And from that, we then are in a position -- will be in a position, I believe -- to define how we make the transition.

And one approach I want to make certain that we do not take is just attempt to do a bunch of things that people think would be interesting to be done. I've seen a lot of technologies already that would certainly be different from what we're doing right now. It's more difficult to find technologies that you can look at and say, "Aha. I know if I do that, I'm going to have a safer country than I have right now."

And so it's really going to be important, and I would hasten to say, in the systems area, we're weak in this area now just because we're building a new organization. We do not have a firm foundation in this area, and it's an area that I'll certainly look to all of you to help us and guide us in directions we can go in to make sure that we improve and do what we need to do.

And then our last -- and this is legislated in the act it created. We have a responsibility to create an enduring research and development capability within the country to support Homeland Security. And part of our job will be to determine what enduring capability means. And so we're working that now.

Dr. McCarthy, who will talk to you about our relationship with the National Labs and our university and fellowship programs, will touch on some of this, I believe, in her talk. But that really is extremely important to us.

Well, other things I mentioned earlier, that we have a number of areas where people help us, starting with the Congress. We also have a number of important documents that we use in order to establish, judge, through our scientific people, where our investments need

to be. We certainly have the Homeland Security Act of 2002. I mean, if people want to know what it is we are trying to do, you can go to that document and read about science and technology. And I can assure you, since it's signed by the President we take it very seriously that that's the major over-arching responsibility we have.

We have a number of national strategies. And also, there are nine Homeland Security Presidential Directives right now, several of which actually influence -- have direct influence on our scientific program in science and technology. There's a tenth one underway right now that's in draft form and deals with bio-security. It will call for a substantially increased role for Science and Technology.

One of the first things I read when I came on board a little over a year ago was *Making the Nation Safer*. That is a fine document -- extremely well-written and high quality. And I can assure you, in my early thinking, it helped stimulate my thinking about what needed to be done and how it needed to be done. And so again, I'm sure those of you who were involved with that effort had many things said to you, but I'd add mine to it, because it's well done.

Also, the Gilmore/Bremer/Hart/Rudman Committees have provided substantial inputs. But ultimately, as we take all these inputs, we've hired, I believe, within the Science and Technology Directorate, some very capable people.

Quite frankly, most of the people that we've hired, if not all, in the directorate are as good as any scientific people I ever encountered, including Bell Laboratories. We've got some very good people who I feel blessed that we've been able to attract. And I think the reason for that is because the mission that we have is such a fundamentally important mission, not only for the country, but also the people that are working on it, that people are highly motivated to be able to be a participant in that, and I'm blessed.

Let me just touch upon how we're organized. For those of you who run businesses, we're a highly-matrixed organization because I could not see any other way to operate this. And the reason for this is that we have technologies that are cross-cutting, all the way from where we need to do fundamental research to direct applications today. And so you pick a technology -- chemical detectors, or whatever it might be -- and that really spans multiple areas in our responsibility.

So we've organized -- and I'm not going to use stovepipe -- with vertical organizations. And the primary four are first plans, programs, and budgeting. You will hear from Dr. Parney Albright later today who will talk to you in some detail about his responsibility and what they do. But it's basically just what I said, plans, programs, and budgeting. He has the direct responsibility for translating requirements from the operational units so that the other three pieces that make up the directorate can do their jobs.

The second organization is the Office of Research and Development. In that organization, Dr. Maureen McCarthy, has responsibility for all of our work with the

National Labs at Livermore, Sandia, and so forth, the major DOE labs that we have direct access to by virtue of legislation that provided such access with the formation of the department. And she also has responsibility for our university programs, which includes scholarships and fellowships, as well as our Centers of Excellence. And we have one of those so far.

She also has responsibility for managing what I'll call the Federal Labs. And right now, there are two of those. One is the Environmental Measurements Lab, which focuses primarily on radiation detection technologies, and that's located in Manhattan. And then we also have the Plum Island Animal Disease Center that's just off the coast of New York. And that organization reports to her and has done so since June 1st.

The third organization we have is the Homeland Security Advanced Research Project Agency. And some people have said it's like DARPA. It has some similarity in that the ARPA is the same. But in terms of its mission and its responsibility it's quite a bit different from DARPA, at least at the present time.

This organization is the primary interface with private industry. And they are letting contracts today with private industry. But at least today, about 90 to 95 percent of the emphasis is on things that can be done now. And what I mean by "now" I mean tomorrow, six months from now, a year from now. By near-term I mean a couple of years. They're working on near-term with only about five to ten percent of their budget dealing with what I'll call forward-looking science.

Now, as we get to the stage where we've got this plan underway to evolve from where we are to where we need to be, then I would see the distribution between long-term scientific endeavor and near-term, that beginning to change shape. But right now, we need solutions today.

And then finally, the fourth organization is one that is called the Systems Engineering and Development organization. And you can think of that organization as when we've made a decision that we are going to go to the field with the final product, someone needs to be responsible for making sure it can be manufactured at an affordable cost, and work those kinds of issues. And that really is going to be a major interface with private industry, because the Federal and National Labs do not take product into final stages of development and manufacture. So it's really going to be a major interaction with private industry in order to make all this work together in an effective way.

MR. VITTO: Since you've organized around these four domains and you expressed an interest, as I did, in the systems engineering aspect of things, while you have a directorate called Systems Engineering and Development, as you pointed out, it's very product oriented and it does get the product to the operational field. So there's a potential danger in that process of too much focus only on off-the-shelf and things that are readily available. Where will the overall threat assessment, infrastructure modeling, understanding where vulnerabilities are, where will that level of systems modeling and systems engineering be done?

DR. MCQUEARY: A very good question. I failed to mention one very important part of the organizational structure and thank you for asking that question. I said we're a highly-matrixed organization and then proceeded to describe stovepipes. We have what are called portfolio managers that have the responsibility for cutting across all four organizations to do the job that has to be done. So, for example, we have a biological portfolio manager. Similarly, we have portfolio managers for chemical, radiological, and so forth.

And then we also have a portfolio that deals with threat vulnerability and threat assessment, which gets right to the heart of what you asked about. And that group of people works not only within the S&T organization, but also directly with the Information Analysis Infrastructure Protection organization that has the first-line responsibility for the IP part of what we do.

So we provide scientific capability, some work we've done in providing threat models for them as a part of the work that they have to do. But we have some people that are in direct residence with the IAIP people working with them to provide them scientific input.

MR. VITTO: And that organization that's doing the specific threat modeling and infrastructure modeling is located where?

DR. MCQUEARY: The people that are working on a day-to-day basis spend most of their time at the complex in Northwest D.C. The Science and Technology group is actually located in Southwest D.C. And so we're a 20-minute ride to get there. But we do have people that are essentially full-time located in residence with the IAIP people because it's important to have the interaction.

Some of the things that we accomplished within the last year we did set up a biological monitoring system called BioWatch. If you've seen that mentioned it's a capability that we've done jointly with the Departments of Health, as well as the Environmental Protection Agency, in those cities where it's located that has environmental air quality sensors at many locations.

And what we did was, in effect, put our BioWatch sensors at the same location as the EPA air quality monitoring sensors are. We take biological samples on a daily basis and make a determination as to whether anything has been detected there. It is time consuming and I think all of us would likely agree that when you're dealing with a biologic threat you're dealing with a temporal threat, because timing is everything, so a major emphasis for us is to shorten that time period.

And our concept is that we would have a sensor at a location that senses, does the assay, and telemeters the information to some central location saying there has been an event at that location, and it is time to put in place what I would hope are already the preventive measures that we need to be taking then.

In this system that we have, we have multiple sensors at each one of the major cities. We monitor on a daily basis. We have had at this stage more than half a million samples that have been taken by these monitors that have been checked. We've had no false alarms. And no, we don't have them turned off to avoid the false alarms.

We've actually made detections in a city where we detected tularemia on a couple of different occasions at multiple locations. We were able to take detections that we made and actually take some of our plume modeling capability in which we were able to make reasonably good estimates as to where these pathogens could have come from. And we've actually pointed possible solid waste storage areas that could be the source.

So the system has worked well. We've had no terrorist-based events at all in which we picked them up. But the system is working better, and indeed, it's worked well enough that in the fiscal year '05 budget, we expect to actually double the number of sensors that we have, and the associated work that goes with them.

We also have a system called PROTECT. I don't recall off the top of my head what the acronym stands for but it's a chemical detection capability in the subway system in Washington, D.C. We have chemical detectors at a number of different locations. There are also cameras around so that if an event happens the information is instantly sent to the central control area in Washington, D.C., the Washington Metropolitan Area Transit Authority, in which people then can decide what kind of actions need to be taken based upon what they see. Because you can see if people are starting to fall over – the first indication of some kind of a chemical attack – you can make decisions as to what needs to be done.

We also have our plume modeling capability from Lawrence Livermore tied into this so that if an attack occurred in a subway station, within about 30 minutes we can make educated estimates as to where a plume of some sort might actually drift, and therefore, aid in determining what kind of evacuation procedures might need to be put in place.

Now, this is obviously just in one area. It's not the whole country. But I think the important thing is we have been able to demonstrate that the system seems to work well. We've had no fundamental problems with it. Its greatest problem, I suspect, is the cost is about a million dollars per station to do this. And Washington, D.C., has its challenges as far as budgets are concerned, and they have paid for a substantial part of that.

In New York, at the Port Authority there, we've had radiation and nuclear warning systems actively working in that area. We have not made detections of any known real threats there. We have demonstrated that such systems can work.

We've generated interoperability guidelines to help local and federal public agencies communicate better. These are just standards and so we're not providing equipment as a part of that. But an important first step is providing standards.

We have issued the first 100 Homeland fellowships and scholarships. That's 50 undergraduate and 50 graduates that we have. And we were very pleased to get that program started in September of last year, and we'll be identifying our next 100 fellows and scholars over the next couple of months.

We established our first university-based Homeland Security Center of Excellence at the University of Southern California, with the focus there being on studying the consequences of terrorist threats, both economically as well as psychologically too. So there may be some opportunity for you to look into that as your interest develops.

The budget for fiscal year '05 as proposed by the President for us in Science and Technology is \$1.04 billion dollars, which is about a 14 percent increase over what we were in FY '04. But that \$126 million increase, about \$65 million of it will go towards increasing the BioWatch capability, and another \$34 million, I believe, is associated with a bio-containment building that we're putting at Fort Detrick. So we'll have that \$34 million, plus an \$88 million that we had from fiscal year '04 will be used to construct a building there that will be our building to be used for bioterrorism types of scientific investigation.

Cyber security is probably the area that is one of these words where if we all said, "I'm going to write down cyber security. Each of you, please write down what it means to you. We'll collect the papers, and we'll read them, and they won't all say the same thing. "

It's a hard problem, first of all. But trying to frame the conversation to have about the problem is a very challenging one that I found myself tangled up yesterday in the Congressional questions. Because it's very difficult to describe what it is we're going to do that we can point to and say, "I know if I do this that we're going to have a safer, more secure cyber infrastructure than what we have."

And, of course, we do have the National Cyber Security Center that reports in through the Information Analysis Infrastructure Protection Directorate. And our job in Science and Technology is to support them. And, quite frankly, we're working the issue daily to try to determine exactly how we make that relationship work. So I would welcome any professional thoughts and insights and guidance that you might have in helping us frame the issue in such a way that we can have a public discussion about it, and then be able to have a conversation that is meaningful to all participants about what we're actually doing.

In the aviation area, we were assigned the responsibility for doing the development work for the shoulder-fired missile threats that we view are possibilities for aircraft in this country, as well as around the world. That program is called a counter MANPADS, Man Portal Air Defense System.

We awarded three study contracts to contractors earlier this year and we expect to have demonstration models available in fiscal year '05 on what we view as a very aggressive schedule. Although there are those in Congress who would say, "Why don't we do it

tomorrow? Why don't we just pick what's being done on military aircraft and use it?" It's a much more complicated problem than that.

And, in fact, when we issued the study contracts, we told each contractor, "If you want to do it faster, just tell us how you're going to do that. We'd be interested in having that conversation with you." And none of them said, "We'd love to do it. We can do it in half the time," or "next week," or whatever it might be.

So it's not an easy problem. Because on commercial aircraft, you have a different set of requirements in order to verify the way the system works.

Well, I'm nearing the end of my preliminary remarks. But I think we've already talked about what your role is. General Welch talked about the four subcommittees, so I won't touch upon that, since you've already done it. I've touched upon a couple of things that I think is of interest to us.

One of the areas I would mention also that will have a lot of interest is in the whole issue of privacy. There is a huge issue in this country of how much information can be made available, how much information can be looked at. And so I certainly, as we go forward in deciding what kinds of areas are legitimate areas for us to be working in, certainly your advice and guidance on the privacy-related issues would be very helpful to us.

An area in which I have the responsibility on behalf of the department is to consolidate in some way the research and development activities within the Federal Government. Not only within the Department of Science and Technology, but also somehow get our arms around -- and when I say "consolidate," I do not mean transfer it in. That's not what it means -- but somehow determine all the related research and development work that's going on within the Federal Government, and try to help make sense out of it. Making sense out of it means it's relevant to what we're doing, and we don't have duplication of effort in multiple areas. And so I would welcome your help and guidance in deciding how we're going to do that, because I don't know just exactly how to do it.

We do have, working relationships at the working level with people in all of the relevant agencies. But what does it mean to provide consolidation in some meaningful way that could be looked at with favor by those who would evaluate what we're doing?

With just a wrap-up, one thing you may or may not know and may recall, it was exactly 11 years ago today that the World Trade Center was first attacked, in which we had six people killed and a thousand people injured. And so here we are 11 years later. It was eight years after that that the World Trade Center in New York was attacked again and destroyed.

And so the threats to our country are those that are people who are willing to wait long periods of time. And one of the concerns, I think, that we all need to be aware of and concerned about is how do we keep the level of readiness up in this country to deal with the issues we've got? Because American people, us being typical, have short attention

spans when it comes to staying focused on something, unless there's a continual reinforcement, some way of making it seem to be relevant. And when nothing ever happens, people can lose their interest.

So I think anything that we can do -- again, along the points that you made, sir, earlier -- about how important it is to be able to engage the American people. Because in one talk I gave, which is nothing profound here, but every American citizen represents a sensor and a communication channel. And so somehow, we need to get American people engaged so that they feel that they're a part of what needs to be done, and not just sitting back and waiting for the Federal Government somehow.

The Federal Government cannot solve this problem. Homeland Security is not a federal problem. It's a national problem that's got to be dealt with by people throughout the nation and agencies throughout the country. And our job is to try to help provide motivation, guidance, and direction that can be implemented in many different areas.

Again, thank you for being a part of this. I appreciate your indulgence in listening to me for the period of time you've done that at a time when lunch might taste better. But I am very much looking forward to the interaction we have, and I hope I have a chance to get to know each one of you well, and understand what your own points of view are, and what you think we should be doing.

Be assured we are going to be listening to you. And whether we can implement everything you tell us to do, I don't know. But I can promise you that I'll tell you directly. When you're telling us what you think we should do, I'll tell you if I think it's a good idea, I'll tell you if I think it's a bad idea, so you won't have to wonder. I've served on committees before in which you provide recommendations. The recommendations go on a book on a shelf or something like that. We're not going to run this committee that way. We will either agree with you and do the things that you said we should do or we'll tell you, "We don't think that's the right thing, and here are the reasons why we can't do it."

But we'll make sure that we do react to the work that you've put into this. Because it's important, and you're giving very valuable time, and you deserve to have a response from us based upon the input you give us. And we will do that. Thank you.

GENERAL WELCH: We'll pick up lunch and continue with a roundtable discussion during lunch.

(Whereupon, a brief lunch recess was taken.)

GENERAL WELCH: We want to welcome Lillian Borrone, who has joined us. And Lillian, everyone else took a few minutes and described who they are, and what they're interested in, and their experience. I invite you to do the same.

MS. BORRONE: Thank you very much, and good afternoon. I apologize for not being able to join you in the morning. I've been chairing another meeting here in Washington. And I apologize in advance, because I'm leaving to go to another session on something else tomorrow, so I will be only here a few hours.

My background is in transportation, management operations, policy planning -- a variety of things. I've had a transportation career that spanned about 35 years in transit, maritime, aviation, what might be called generally intermodal transportation, as well as in running significant transportation organizations.

I retired at the end of 2000 from the Port Authority of New York and New Jersey as assistant executive director. Prior to that, I had been the port director for New York/New Jersey for about 13 years and have been very involved in both international business development and regional economic development activities. This is largely because I, as part of my role at the Port Authority, ran the overseas offices and the development of businesses for the New York/New Jersey area in international commerce.

I am a member of the National Academy of Engineering and also have been an active member of the Transportation Research Board of the National Academies. And, in fact, I had the honor of being the first female chair of TRB in 1995 and 1996.

I am also currently a member of the U.S. Commission on Ocean Policy. We were authorized by a Congressional act in 2000, and we were appointed in 2001 by the President and the Congress. We are looking at all of the federal policies and laws and regulations that govern our activities in the oceans, whether they are environmental, military, economic, dealing with climate, dealing with research, or dealing with education. That body is chaired by Admiral Watkins. Its goal is to make recommendations to the President and the Congress this year. Our expectation is that we will have a report concluded by June. It is about ready to go to the Federal Register next month for comment by the federal agencies, and the governors, in particular, but anyone in the country who wishes to have one otherwise.

I also, in my retirement, am on a number of boards. I chair the ENO Transportation Foundation here in Washington, which is dedicated to framing emerging transportation issues and cultivating leadership in the broad transportation sector, not just in a particular modal interest area. And I'm on a couple of other private sector boards.

My interest really is in transportation operations management and policy, with a particular focus on security, but not solely. While I am described as a transportation security expert, I don't think of myself narrowly that way. I really think of my role as one of looking at the broader issues and trying to make sure that transportation functions in an appropriate way, incorporating the security concerns in the fashion that it needs to.

My specific experience after 9/11 running recovery and victim assistance for the State of New Jersey and working as a cabinet officer for the Governor on setting up our security task force and dealing with the business community and the transportation community

really helped to crystallize some of the issues that I think we are likely to deal with in terms of how we use technology and how we help the, from my point of view, transportation community, and in particular, the economic commercial aspects of that community, incorporate those technologies and enable DHS to better function is sort of the area that I'm not only curious about, but interested in helping to better define.

A lot of that interest stems from the work I had done as port director, working closely with the Coast Guard and other agencies in trying to find ways to better leverage the resources that we were committing to development or to strategic directions that were diminished, because there wasn't enough resource committed or because multiple agencies were overlapping and not achieving the kind of consistency and weight that I felt that they could achieve by working together.

So in my work with Admiral North and others, I was able to help bring the communities together through leadership positions I held in that era.

I think I can bring some experience, but I also think I can bring dialogue back to the industry community. I spent yesterday afternoon with an assistant secretary at DOT exploring whether they have been thinking about what DHS is looking at in terms of how they might interpret it for operational policy-setting and strategic implementation. And they really haven't to the degree that I think we need to see that occur.

So that's my long answer to your short question.

GENERAL WELCH: Thank you very much. You described a complex set of subjects.

We have time now, having digested Dr. McQueary's comments, to explore further. I have one question, and that has to do with how you see the role of the National Laboratories, first as it applies to DHS. But also, if you want to make a comment, since you suggested that one of the larger things that somebody has asked you to take on, which I would regard as formidable, is to look at the overall coherence of federally-funded research and development. But first, the kind of relationship and what kind of role they need to play for DHS S&T.

DR. MCQUEARY: There are actually nine National Labs that are relevant or potentially relevant, some more than others, to what we are doing or want to do. As some of you may know, we would identify labs that would be designated as intramural, meaning that they were going to have access to everything that we do, and therefore, would be insiders. And then the others, we would designate as extramural, and they would compete. What we were trying to do -- what we thought we were doing -- was make it maximally possible for each of the labs to be participants in our activities.

Well, without anyone really trying to understand fully our intent -- or at least that's my conclusion, although there are probably varying views -- we started getting a firestorm of Congressional criticism for having taken this approach.

So the bottom line is that we have agreed to have an independent group take a look at the criteria that we used for making this decision and taking this approach. We're going to do this over the next months or so.

With that as the backdrop, the labs are fundamental to our ability to be able to do the research and development work that we have to do. There's no question about that.

Right now, we have a memorandum of understanding signed by the Secretary of the Department of Energy and Secretary of the Department of Homeland Security that spells out that we can have free and open access to those labs.

An open issue, one that's not quite worked out, is exactly how we gain entree into the labs. DOE's preference would be to have that be through them. What we would prefer to have is our own direct contracting relationship with the lab, so that has to be worked. Anything you can do to help us move it in that direction, I think, would certainly be welcomed in that regard because we clearly do need to have a relationship.

The key issue, I believe, if you take a look just in this year, if I can use that as an indication of where we are, the nine Labs that I mentioned have close to \$9 billion. The amount of money the Department of Homeland Security will spend is \$300 million with the labs, and a hundred million of that is just helping Borders and Transportation Security do some work. Only \$200 million will actually come out of the Science and Technology Directorate.

So financially, we don't have much leverage at all. We need to make sure that we can get access. We need to make sure that we're not just a "when they don't have anything else to do, they'll work on our stuff," because we can't be dealt with in that way. And I don't mean for a moment to suggest that I feel that that's the way we're being treated, because we're not. They've put some very talented, very capable people to work on our problems. And we have a number of people that are on loan to us from the labs working with us, since it's an important resource there.

So this working relationship is very important. We'd like to have our own direct contracting relationship with them. I think that's the way to make sure that we are getting the attention that we need. But we need them, and I'm satisfied, at least, the way the relationship has been going so far, with that one little nuance.

GENERAL WELCH: There's another agency that has a name that sounds an awful lot like what you do, and that's the Defense Threat Reduction Agency. What kind of relationship do you see with them?

DR. MCQUEARY: We have a pretty good relationship. We've run some joint exercises and done some plume modeling work in Oklahoma City late last year, which was a joint activity. We have, essentially, a quarterly meeting with their folks at the senior level -- Paul McHale and Dale Klein -- to stay coordinated. And, of course, DTRA reports to Klein.

DR. ROCA: Dr. McQueary, you've scaled the problem earlier. There are millions of transactions a day with error rates that have to be 10 to the minus a lot. You've got any number of threats that are almost too long to list. There has to be some process for prioritizing what one does, other than the squeaky wheel one, of the loudest voice driving you on a given day. Have your folks been able to make any progress in coming up with some systematic way of identifying the threats and prioritize them?

DR. MCQUEARY: To a degree. And this is still being refined, you know, every time, and it really translates into where we spend our money. And I talked to someone at the break about this.

There are really two significant factors when we start looking at how we're going to make our investments. One, you look at what the consequences of what the event would be, or whatever that terrorist activity might be. And certainly, nuclear, there's a huge consequence if we had a nuclear weapon go off in this country. Biologic events have great consequences. Many of the others are certainly much less in terms of number of people that are killed.

Another factor, though, in terms of determining what the investment would be is the likelihood that the event would occur. And if you look at the likelihood of a nuclear weapon being set off in this country, there is a very low probability that that will happen.

The likelihood that someone or some people could do great damage to us in the biologic area is extremely high, because there are so many different venues that could be used, the ease with which things people could make, the distribution of, whether it's animal sicknesses, or human, or plant. You name it. It's a pretty straightforward, easily understood thing to be able to do. And therefore, the biologic area receives about 40 percent of our funding just based on the logic of thinking about it. I don't know if that gets to your question, or gives you an answer or not.

DR. ROCA: If I might continue. Even though at the next level of detail, you can introduce biological agents via the postal system, as we've discovered. You can introduce them through couriers. You can infect an individual. There are probably, you know, hundreds, if not thousands, of ways. I'm wondering more to what extent do you feel that the department has got a process in an ordered fashion attacking these issues?

DR. MCQUEARY: I don't think we would have something we can hold up to you and say, "This is our process." I think this is really -- it's an evolutionary issue. And right now, we've taken the various areas that I mentioned in looking at what we're supposed to be doing. We've hired a lot of smart people. And fundamentally we base our decisions on the efforts of these people. And Parney leads the effort on deciding where our budgetary emphasis is going to be. But this is done through a lot of conversation and discussions among the scientific staff that we have, and the expertise that they have in helping guide us as to where we're going to go.

Of course, the bottom line budget, if you will, is pretty much predetermined in advance. And so we work with that.

But I also hasten to say that I feel uncomfortable with the budget that we've got right now, or the budget that we had for the last three years, part of fiscal year '03 and '04. Because to date, we do not have an effective way of identifying the consequences of what we're doing in a quantitative way.

And I touched upon this earlier. I think it's very important to be able to quantify the improvements that we make as a result of the scientific investments we make. And we've got a ways to go, a substantial ways to go, to be able to really do that in an effective way. Some areas probably do it better than others.

We ultimately need to be able to say, in a way that can be explained for lay people to understand it, "If we do this, we're safer. And here are the end reasons why we are safer," in a way that people can relate to and understand.

DR. SHINE: Two questions. First, you emphasized the notion of sustainability. There are a large number of threats, only a small proportion of which are likely to actually happen. This situation raises the whole question of strategic investments in S&T based on dual use, and the notion that one might want to put one's highest priority. Not that one doesn't fund certain activities that, as you say, are very high risk for a major event, but that you do choose those areas where there is the potential to have an ongoing sustainable effect. And we're talking about biological. Obviously, I'm interested in that in terms of my view being West Nile is perhaps even more important in terms of our ability to recognize it early and to respond to it.

So I'm curious as to what your general philosophy is when you look at the S&T agenda about the notion of dual use, and how much that influences your thinking about where those investments ought to be.

The other much harder question is in your outline of activities, you described an activity in risk analysis. My question is where is the research agenda under S&T on risk communication which is, it seems to me, a different set of research questions of which Baruch has obviously made some reference.

DR. MCQUEARY: I'm going to let Parney take a shot at that, since he's been at this longer than I have, and had a more detailed involvement on a day-to-day basis.

DR. ALBRIGHT: Generally, when we make our investments and decide what it is we're going to do within the department, we tend not to initially ask the question is this something that is going to have, for example, public health benefit, or, you know, benefit the cop in the field, for example, for other reasons?

And the reason for that, of course, is that, you have to set your priorities based on what you perceive the terrorist threat to be. And the fact that something might have particular

public health benefits is not going to be the initial focus you take in determining what it is you're going to do.

However, having said that, deciding what specifically to do in a particular area -- for example, sort of a classic area to think about is medical surveillance technologies and information infrastructures, where clearly, once you decide that is something that's worth doing, from a bioterrorism point of view, you would then be foolish not to build into it the hooks and capacity that would allow it to be of benefit to the greater public health. Because as is implicit in your question, if it is of day-to-day benefit, then you'll sustain the investment over a long period of time.

But I will tell you that there are several things that we're doing within the department, radiation detection at the borders is a good example, where it's kind of hard to come up with a reason for doing that, other than to prevent the importation of a nuclear weapon into the country.

DR. SHINE: Hazardous chemicals, for example, is a dual-use area.

DR. ALBRIGHT: Sure. The point is where you can leverage things. And clearly, if it has a dual use, then you know it's something you want to do because you can sustain the investment.

You know, again, in the medical surveillance arena, you can get -- I mean, first of all, there's a mundane issue. You can get CDC to pay for it instead of DHS, which is a good thing.

But, it also has advantages to public health. We are in the process -- the President has got an initiative in bio-surveillance that he just put out in the most recent State of the Union address. And, we're interested in early detection of things like infectious diseases that aren't necessarily aerosolized. Things like smallpox.

Having said that, we're also going to be tracking every flu epidemic that comes through, every kid, every virus that, you know, goes through the elementary schools. Everything will be tracked. And we're going to get data and information out of this. We're going to get science out of this that we've never had access to before. So it will be interesting to see how that works out.

The same thing at the borders. We're making significant investments at the borders that we have never made before, because the problem was not perceived. INS has a long history of little pilot projects they've put up along the borders and Customs has a long history of doing this and other projects that never got carried through to fruition because no one was willing to make the investment. And the reason no one was willing to make the investment is because it was always below the cut in terms of priorities.

Well, now, Homeland Security has come along and raised the bar basically put these issues above the line. But now that they're above the line, it is now possible to make

investments at the border that not only make the country safer, but also expedite travel and make things more efficient.

Some of the things we're doing in terms of U.S. Visit, for example, have the potential of expediting people more rapidly through immigration. And we have the potential with things like the Container Security Initiative and things like that of getting the vast majority of the traffic expedited through the borders, as opposed to being randomly searched.

So there are certain advantages along those lines. These are, again, investments that would have led to efficiencies that just no one ever felt were important to make.

Now, going to risk management or risk communication. That's something we talk about a lot. It is something that, as you know, is a vexing problem. The idea of how does one communicate low-probability events to the public has always been a struggle. I mean, there are textbooks written on this.

And the answer to your question is no, we don't have anything in the pipeline in terms of a research agenda. There has been some talk about a potential one of these Centers of Excellence being focused on that. We haven't really made a decision on that yet.

Our public affairs people, Susan Neely and her staff, have been putting together an initiative to educate the media on risk, and educate them on some of the things that Dr. McQueary has been talking about, things like radiation and biological threats and that sort of thing.

But how does one, for example, communicate to somebody after an RDD has gone off what it really means when you say that the probability of their cancer risk has increased by one part in 10^5 ? What does that mean to people? That whole communication thing is something we're very concerned about, but we don't really have any good ideas, and no, we don't have a research agenda on that.

MR. FERREN: I think the words before lunch were very compelling about moving quickly and getting things out there that actually do our people good quickly. However, in my observation, large organizations in general, and federal procurement in specific, you seldom hear the words "quick" or "efficient" mentioned in terms of time domain on those classes of organizations or procedures.

I'm wondering if the department, and S&T in particular, has a strategy for how to move quickly within the constraints of large organizations and federal procurement regulations, which are really designed to make sure that doesn't happen.

DR. MCQUEARY: As a part of the Homeland Security Act, we were given some latitude in what we could do in terms of contracting. And let me illustrate by example what I mean by doing things quickly.

I talked earlier about the counter MANPADS work that we did. We actually put out the RFP in October and had the proposals in -- more than three, I think it was five or so, maybe more than that, and then we pared it down to five, and then down to three -- and we awarded our first contracts in early January. So it took us about three months from start to finish on that.

Now, we had people that were knowledgeable to be able to write the proposal. We had broad agency announcements that came out in late October or November. And we're issuing contracts now. We started a new Small Business Innovative Research Program just last month. And already we have proposals in. We have 66 we've chosen to be awarded. The contract negotiations are under way for that.

So with the latitude we've been given, we at least can make it move. Whether that latitude will stay there long-term or not, that remains to be seen.

But the way I've described it before, I cannot conceive of a situation in reality in which if we know from a scientific point of view what we need to do in order to make the country safer, and we say, "Well, it's going to take us seven years to procure it," I mean, that's a conversation one should never have to have. So we've got to be able to move it. I think what we have to do is every moment, step on those cases that seem to be getting in the way of moving quickly.

And I just encountered one a short time ago. We made our choice on our first Homeland Security Center of Excellence back in November. And the bureaucracy got in our way that we just finally got the money out to them yesterday or the day before. I mean they had \$5 million coming to them. And from my standpoint, if I say we're going to spend it, we made the choice, why should it take so long to do that? And I don't know the answer to my own question right now, though I'm going to find out. It doesn't make any sense to me that the system should be so cumbersome.

Perhaps one thing could be said. Better men than I have tried to solve that problem and failed.

MR. FERREN: Well, it seems that in large organizations, nobody has the ability to say yes, but anyone can say no.

MS. BORRONE: I'd like to ask Parney a follow-up on that last answer. As you see the opportunity for dual-use results products, are you involving the other federal agencies who may be the beneficiaries of these products up front in the framing of the research agenda? Or is it that you're informing them en route, and hoping that they translate it into useable forms? That's the first part of the question.

The second is I noticed in Dr. McQueary's testimony that there is a review going on of the R&D that's taking place in the federal structure. Can you give us some sense of the time frame for that product?

DR. ALBRIGHT: The answer to the first question is yes we do involve other agencies from the get-go. You know, again, on the borders and transportation side of things, clearly, there are some interactions with DOT that are obviously relevant. But a lot of those activities are now part of the department, especially the border issues.

Regarding, the bio-surveillance thing that I mentioned earlier, we meet very frequently with Julie Geberding and the CDC folks. They're the ones who have the responsibility for medical surveillance. That particular initiative involves much more than just medical surveillance. It involves agricultural surveillance. It involves food poisoning reports, EPA types of things, and all those people are playing a role.

As far as review of the overall RDT&E for Homeland Security within the Federal Government, we have a responsibility in Section 3022 of the Homeland Security Act to develop a national strategy and plan for research and development for civilian Homeland Security RDT&E. And we're not there yet. There are a couple of issues associated with that. One is an authority issue. We have a statutory responsibility to do that, but we still need to get executive authority to basically take the lead on that. And that's something we're working through with the White House and how to make that happen.

Secondly, that kind of coordination happens basically through the standard processes that exist within the White House, through the Homeland Security Council, OSTP, etc. There's an NSC counter-terrorism R&D activity. And I would say that we are very cognizant of what's going on in things across the Federal Government. But still you never know what you don't know. I wouldn't be surprised if I walked into a room somewhere and found out about something I didn't know about. But I think we've got our arms around almost all of it. In terms of creating a national strategy, I would say we're probably three or four months away from doing that.

DR. GAST: Dr. McQueary, I think everyone would agree that you listed a very impressive set of accomplishments, especially in such a short period of time. It's very comforting to see so many things started. And also, I think it's laudable to have set up a matrix-type organization. I guess my question is really how well you are able to, at these early stages, really integrate your portfolios and integrate your projects. I was struck by the nice descriptions of BioWatch and PROTECT being very exciting technologies and exciting things that will protect the public. But in both of those, you mentioned their immediate communication and immediate transmitted data to another location, which is obviously a very important piece of their functioning.

And so if I take communications and cyber security, which sounds a little fuzzier and less well-developed, my concern is how are you able to get portfolio managers focusing on these areas to really cross boundaries and think about "This won't work unless we can transmit the data"?

DR. MCQUEARY: I think at least a partial answer to the question comes back to a point I made earlier. I don't think we've done a very good job of getting the systems engineering responsibility that we have to pull all these things together. We have pockets

of capability and successes we could point to. BioWatch, I think, is a good one. I mean, it's almost a stand-alone system, but it does have to interact with a number of different agencies and so forth. So in that sense, it works well.

But to address the root of your question we've got to have a larger overarching system engineering capability, and I think we believe within the directorate the formation of the Homeland Security Institute will provide us the talent base that we will need in order to do a better job of addressing that issue. But you raise a very important point, and I agree, I believe, with the thrust of it.

DR. GAST: And the integration of the people up to a certain level in that area, not just to rely on yet another expert to bring on the integration.

DR. MCQUEARY: I'm missing the latter point.

DR. GAST: I think part of it is educating and teaching people to think beyond their portfolio, and learn their own means of systems integration from the systems integration experts.

DR. MCQUEARY: Right. Well, keep in mind, we have chosen who the portfolio managers are. And so I believe Dr. Albright has done a good job of selecting people. They're not only experts in their scientific areas of endeavor, but also people of great leadership skills to be able to do, I believe, at least some part, if not a substantial part, of the point that you're making.

DR. PAPAY: A comment and a question. In fact, the comment may be a question. As a follow-up to *Making the Nation Safer*, the National Academies have been doing some work in threat assessment risk analysis, and that report is fairly close to completion, I think, at this point. I don't know if you've interacted with them at all on that. But I'll give you a heads-up that there is one that is coming, and I think it could be used from that point of view to help to quantify the approach.

The question gets to what I'll call the bureaucratic cracks. And one area of particular interest is you tend to talk about what you can do at the borders, and perhaps to points of embarkation in terms of containers, et cetera. But using one specific example on nuclear weapons, especially technical weapons, rather than strategic weapons. There's obviously a lot that can be done upstream to be able to eliminate or reduce that threat. But you talk about the civilian population, civilian threats, et cetera.

What are the mechanisms to be able to move upstream in terms of some of these threats? That is, to go beyond our borders and address issues? Obviously, State Department, Defense, and some other agencies are involved. Can you give us a flavor of where you are on those approaches?

DR. MCQUEARY: Most of the interactions that are going on in the areas you just touched upon are being done outside of the Science and Technology Directorate

responsibilities; although I'm sure we have people that are intimately aware of what's going on.

I think to characterize the point that you're making, we must, as a Homeland Security department, do a better job of finding out things before they get to our borders. Because once they get to the borders, we're in a defensive mode. And when you're in a defensive mode, you tend to make more mistakes than you do when you're in an offensive mode.

And so we have to continue to work the issue of what we do in order to know that what's coming towards the borders. And certainly in the container security initiative, that the borders and transportation group has had underway, that attempts to make some steps in the direction of addressing the container part of the problem.

DR. ALBRIGHT: Let me just comment specifically on the nuclear one, because you brought that up. The Department of Energy has the MPCA Program, as I'm sure you're aware of, which involves safety and security of the actual source material, from the Soviet Union, primarily. And then, of course, there's the second line of defense activities that occur in the former Warsaw Pact countries.

You know, there have been a lot of issues associated with that problem. As you know, DTRA has a piece of that, State has a piece of that, and then DOE has a piece of it. Although I will say that all roads end up leading to DOE on this one, eventually.

That's gotten a lot better coordinated than I think it was a year ago. There was a GAO report that Senator Roberts commissioned that was very critical of the overseas programs.

You're exactly right, if you're going to control physical materials, absolutely the best way to do it is overseas. The goal-tending is something you prefer not to get into. That doesn't mean you don't have to have it.

Now, having said that, the Department of Energy has not invested a great deal in research and development activities associated with those activities. The biggest investment they've ever had in terms of improving sensor technology, for example, was \$10 million in FY '03, and that was a plus-up they got after September 11th. Typical investment for R&D in those activities was \$2 or \$3 million a year.

We've got \$129 million invested in rad nuke RDT&E in Department of Homeland Security, of which about \$60 or \$70 million -- I forget the number -- is specifically devoted to pushing the football a little bit further down the field in terms of sensor technologies.

So one of the important things for us to do as we go on that big push is to make sure that the things that we do are consistent with what the second line of defense might be able to use.

Now, as you know, they've got to buy it from the Russians as part of the treaty. So there's a lot of policy issues about how do we transfer this technology, how do we get it out overseas into the field. But nevertheless, that's something we work very close with.

By the way, that's a place where the White House coordination process really works well. There's actually a joint NSC/HSC Policy Coordinating Committee that looks at these issues that we participate in very heavily.

DR. FISCHHOFF: I guess I'll also take us downstream with a comment, and then a question. The comment is that I actually think the science gives us more reasons for optimism regarding our ability to communicate with the public than an audit of communication failures will show that they're often on the part of the transmitter rather than the part of the receptor. So I think that's actually -- I think that's probably more tractable.

Particularly where this comes up from the example that Parney mentioned earlier, I'm interested to know how the agency -- how the department deals with it -- this is a downstream question -- that we will have -- you know, if there are incidents, or there are even just serious false alarms, we have an issue of clean-up standards, or decontamination. And if we're thinking of what are the impacts in terms of the economic impacts and the social impacts, you know, contaminating a large area to a very low degree will be a significant disruption. If we wait until it happens, and then we have to decide well, are we going to clean these up to our traditional standards that grew out of the nuclear power industry, you know, for a tiny risk.

So how do we deal with achieving these standards. I think from a public health -- it's probably a scientific question. But I suspect from a public health perspective, getting the people back into resuming their lives in weekly active radioactive areas are probably good for their health, good for social cohesion, but it's going to be harder to do when people are stressed afterwards, and there's issues of trust and so on.

So there's partly a scientific question, but there's also a policy question. I just wonder how the department organizes around these kinds of things.

DR. MCQUEARY: Well, I wouldn't say we're organized around it, but certainly we're intimately aware of the issue. And the differences I think you're describing is the difference between, for example, what EPA environmental clean-up standards might be versus what is an acceptable level of whatever the contamination might be. There is a disconnect.

An area that we have a lot of concern about is what happens if we have an event. Because if the Federal Government then comes in after an event and starts trying to explain this away without having agreed among itself various components what the acceptable levels are, there will be a great deal of distrust in the American public, I think, inevitably, because it comes about "What's the Government trying to do to us now?"

So we are a part of discussions with EPA and others on the issue of how do we reconcile these things? And how long it's going to take to work through that, I don't know. Because I'm told there are instances where the radiation background in Denver is higher than the clean-up standards that we might have to be faced with if we follow EPA standards. And that, obviously, is not an answer -- the people in Denver are not clamoring to have the environment cleaned up there, as I understand it anyway.

Anything you want to add to that? It's an important issue.

DR. ALBRIGHT: We're working the problem very hard. There are a lot of authority issues that are involved -- you're right. The policy issues here are transcendent. You know, who makes the call?

There's also a fairly stiff regulatory environment that exists. You know, there are agencies -- Department of Energy, for example, surprisingly, has a lot -- I mean, they have a lot invested in terms of their regulatory environment in a particular set of numbers that they have to clean their labs up to, for example. And so there are a lot of bureaucratic issues here about what the right thing to do is.

And maybe when we go to the classified session, we can talk in a lot more detail about it. Right now, we're in a situation where you have absurd results, you know. You would be cleaning up an RDD in Washington, D.C., to a level lower than the national background in Denver, for example, based on EPA standards. So we're obviously working that very hard.

DR. ATLAS: I would first add to that the academy has an ongoing study on how clean is safe in the bio area, which is really complicated by the fact that we don't have the standards especially set out there.

But the question I was going to ask, I was going back to your description, sort of the vertical aspects as well as the cross-cut, and the border role of integration of DHS, there must be other scientific advisory boards both on your verticals and maybe on your cross-cuts. And my question is how this advisory board really relates to those in filtering and getting you the right strategic advice.

DR. MCQUEARY: The only formal advisory board that we interact with now would be Secretary Ridge's Homeland Security Advisory Council. And this board will have interaction with Jared Cohen and Dr. Ruth David, who chair and co-chair the Academe and Policy Research Senior Advisory Committee of that organization. I just met with them before coming in this morning. And I think one of the issues for this group to do is to work to decide what your interaction needs to be with them.

The thing I would like to avoid is having two separate advisory committees telling us what they think we should be doing. I'd rather have you act as our go-between between Secretary Ridge's committee. But other than that, I don't think we have any other advisory committees that we deal with.

DR. ATLAS: So the vertical ones, you don't have?

GENERAL WELCH: There are a number of inherited advisory committees. We will get for our next meeting a description of what's there and how active they might be.

DR. MCQUEARY: I would not view that any advisory committee that has existed in the past necessarily needs to continue to do so. I'd rather view that this committee will be our first point of contact to deal with advisory committees, and you help us decide what we need.

DR. BESSETTE: My question has to deal with, which you brought up earlier, sustainability of programs. And I wondered, does the department have any thoughts in terms of requirements of matching funds from either private industry for any of the funds that you distribute, or from other states in order to improve that sustainability and improve the leverage?

DR. MCQUEARY: We don't have any policy that I would point to in that regard. However, there's some what I'll call inevitable realities in all this. Eighty-five percent of the critical infrastructure in this country is in private hands. I can't personally conceive of a scenario where the Federal Government says, "It's our responsibility; and therefore, we'll ship money out to all of these private industries."

I think we're in an environment where terrorist threats are a reality of doing business in this country. And therefore, businesses have to step up to the plate and be prepared to deal with the responsibility that goes with having a responsibility to shareholders and board of directors.

And it is also -- along the same lines, it's my view that those companies that move out quickly and position themselves as having worked the issue of protection against terrorist threats will find themselves in a better competitive position. Because if you or I are trying to decide where we want to invest, and you've got two "equal opportunities," one of which is the companies have done a good job of doing the things, whether it's cyber or physical security or whatever it might be, and another hasn't, it's pretty easy to think, "I think I'll put my money in the one where they've done the right thing."

So I believe there is an opportunity in a competitive society such as our own for doing things that improve the protection of one's capability can be a competitively advantageous thing to do. And from my standpoint, that's the way I would view it.

I just don't believe that this is an issue where the Federal Government -- I think that the Government needs to provide standards, it needs to provide guidance, it needs to provide help in certain critical areas, and we've done that with grant programs and so forth.

But ultimately, businesses have to step up to it. And then to the degree that they can, state and locals have to. And then we do have mechanisms in place for the Federal

Government to step in and provide additional funding and support in those areas, particularly in the first responder area.

Whether there's ever enough in any given year, I don't know. I suspect no matter what the size that one might distribute, you can always find one more thing it would be nice to be able to do that year. So it becomes a question of how much the country can afford, to a degree.

GENERAL WELCH: Thank you. For the members of the public who are here, we didn't have time today to receive any oral commentary. However, we appreciate your interest. If you have any comments, you can e-mail them to hsstac@dhs.gov, and we will pay attention to them. Thank you.

(Whereupon, at 1:50 p.m., the meeting was concluded.)

* * * * *