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

February 16 – 17, 2017
Committee Meeting
Location: 1120 Vermont Ave., NW, Washington, D.C. 20005
Washington, D.C. 20005
Minutes

Summary: About 43 people attended the meeting (please see list below). A recording of the meeting sessions can be found at:
Day 1: https://share.dhs.gov/p9l96cbkgor/
Day 2: https://share.dhs.gov/p1pofexe9su/

Day One (*Thursday, February 16*):

1. **CONVENE AND OPENING**

The Homeland Security Science and Technology Advisory Committee (HSSTAC) Designated Federal Officer, **Michel Kareis,** convened the meeting at 1:30 p.m. **Kareis** welcomed the committee members to the HSSTAC Quarterly meeting. She provided an overview of the agenda and notification that the meeting was public and being recorded. The HSSTAC members introduced themselves followed by all of the observers in attendance.

2. **HSSTAC SUBCOMMITTEE UPDATE**

Dr. Ted Willke, Chairman of the Subcommittee on Commercialization, provided an update on the work that has been done since the November meeting. The subcommittee received a letter from Dr. Bob Griffin, Acting Under Secretary for Science and Technology, spelling out the mission and scope for the subcommittee. The commercialization sub-committee is focusing on technology transfer and transition to components and first responders. The intent is to have better life cycle outcomes, requirements, procurement technology and to fill gaps where there are unmet needs.

One ask for the full committee is that if any HSSTAC members know the right stakeholders to reach out to for assistance with the report to let Ted know.

Willke went on to elaborate on gaps. Willke stated that as a recommendation DHS should take a role in setting requirements and facilitating standards to help alleviate some of the repetition. There needs to be more community outreach. In the report the subcommittee addresses the issue of new technologies by 3rd parties and how they are vetted to determine if the meet requirements.

Chief Keith Bryant, Chair, Subcommittee on Social Media Working Group provided an update on the subcommittee since November. The HSSTAC voted to approve the report, *Best Practices from Incorporating Social Media in Exercises*. The purpose of the report is to provide first response agencies with best practices based on case studies and how they can integrate social media into the planning, conducting, and evaluating exercises that they conduct. The final draft will be sent to the Under Secretary for Science and Technology for review.

At the last meeting the subcommittee received a presentation on information system and crisis management response (ISCRAM) an international group that fosters R&D and knowledge exchange, to include social media. And finally, the work that this subcommittee has been doing will be allowed to continue under its own federal advisory committee.

Dr. Vincent Chan, Co-Chair, Subcommittee on Internet of Things Smart Cities reviewed the original charter and objectives for the subcommittee. Chan estimates that there are 30 to 60 billion objects for internet of things. With this there are many security challenges to keep in mind. Resiliency is different than security in IoT. Systems will always be breached but the question is how resilient will your system be? The charge for this subcommittee is: what does the Smart City of the future look like? What are the security challenges? How do we make it more resilient? How would the government compose new applications on top of the richness of the commercial IoT? And what would the add-on R&D necessary for a resilient IoT?

Security is a serious issue for public safety and infrastructure. We must work to protect it especially when dealing with autonomous vehicles, attacks on systems, and the capability of adversaries. We must employ techniques to detect and mitigate attaches and fill gaps in protection. This will involve investing in R&D. DHS could work as a conduit to create partnerships for information exchange and load sharing as time and cost saving measures. Long term security challenges include operating with compromised nodes or assets. Insider attacks are a distinct possibility. Cyber and physical security are increasingly interlinked (power grids, dams, etc.). IoT can be used as an overlay for cyber physical systems but it can also be used against you. Plans for disaster recovery/critical systems restoration must take into account distributed sensor networks and loss of communication systems.

A few recommendations for the government to take to protect the Smart Cities:

- Reach across multiple agencies for coordinated/integrated approach to protect IoT/SmartCity
- Government must develop more focused and secure applications to ride commercial IoT
- Critical gov. review must be undertaken and be periodic to look at deployed sensors
- Government funding for R&D must be increased to improve government-related Smart City needs

- Create governance and operating model, policies, and standards including interoperability' manage processes and capabilities – assessing local, state and federal preparedness
- Risk awareness and culture – DHS must evangelize security to developers and public periodically assessing preparedness
- It is extremely likely sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes
- DHS should articulate and protect expectation management – what the public can expect in a disaster must be made clear
    - Expectations and severity must be described to the public

3. QUADRENNIAL HOMELAND SECURITY REVIEW SUBCOMMITTEE

Jason Ackelson, Office of Strategy and Analysis, presented a request to the HSSTAC to create a subcommittee at the November meeting. The subcommittee has been asked to create Whitepapers on the following topics: Cybersecurity, artificial intelligence, autonomous technology, adaptive manufacturing, and chemical/biological/radiological/nuclear (CBRN). These papers will be presented at the Homeland Defense and Security Education Summit – "Overcoming Barriers: Looking at the next 10 years of homeland security strategies, plans, policies, and planning.

Meeting Open for Questions or Comments from the public:

Question: In terms of the commercialization topic, how does HSSTAC define commercialization, technology transfer/transition, how much of a part does S&T have or what is S&T's role, how much does S&T touch something before it is considered commercialized/transitioned?

Willke responded by saying that there is a role for S&T to play and there are things that can be done, such as looking at full scope in terms of transfers, enabling third parties to build, setting requirements with committees and components, testing and evaluation, supplying IP, evaluating solutions, and setting standards.

ADJOURN: Kareis adjourned the meeting at 3:12 p.m.

Day Two (*Friday, February 17*):

1. CONVENE AND OPENING

The Homeland Security Science and Technology Advisory Committee (HSSTAC) Designated Federal Officer, **Michel Kareis,** convened the meeting at 9:00 a.m. **Kareis**

welcomed the committee members back to day 2 of the HSSTAC Quarterly meeting. She provided an overview of the agenda and notification that the meeting was public and being recorded.

2. TECHNOLOGY SCOUTING BEST PRACTICES

Michel Kareis lead the session to facilitate discussion on technology scouting best practices. The first question presented to the committee was: what are cost effective best practices to discover and maintain awareness of what the following communities are working on with respect to science and technology? (Industry/Federal National Labs/Academia)

Response Summary:

- Partnerships are key, especially with tight budgets. There is enough technology available that needs to be shared with industry, labs, and academia. Having equal "skin in the game" and co-sharing infrastructure will help build respect and proactive relationships. Money matters less than the relationships. Leverage other agency models.
- Create a guide with subject matter experts on hand similar to SAGE (Scientific Advisory Guide for response to Emergencies)
- Hosting Grand Challenges, Gadget Off, and Annual Conferences to find solutions and create more public awareness of what S&T does. DHS prevents bad things from happening but bad things still happen. Invite others to participate in "Best Tools in Response and Recovery" and put them into effect during an event to show case resources and technology.
- Industry Day – rapid fire and effective on what's effective, especially for tactical operations. Attend Vendor Conferences to see what is going on. Spread money into small bets with academics and have them write good reports on the big events
- Centers of Excellence (CoEs) are very valuable. They have evolved to be a safe space from regulators, government, and nexus to allow for conversation that otherwise would not happen.
- Relationships matter. Universities are big mayors of large populations. They can act as conduits to accomplish your mission.

What are effective mechanisms to communicate to industry what capabilities (to include products, research, prototypes, etc.) S&T is interested in learning about, when our turnaround time is 3-4 weeks?

- Move away from "stovepipe sciences". Facilitators and softer science can help, learning systems to incorporate into other businesses or technology.
- Adopt a risk based approach with a capability focus - Look at Scope. How do you quantify cyber tech effectiveness? How do you measure your effective investment? Assess the capabilities. How does one scale that capability?

Comments from the Public:

David Olive commented that Safety Act has the most private sector outreach. S&T works with companies to develop anti-terrorism technologies. He wanted to

emphasize the success of the partnerships

3. TECHNOLOGY TRANSFER AND COMMERCIALIZATION BEST PRACTICES

Michel Kareis lead the session to facilitate discussion on technology scouting best practices. There were four questions presented to the committee:
1.) What short and long term impact, if any, has the new Administration had on the way domestic and international technology companies are doing business?
2.) How will those changes impact technology development and commercialization?
3.) How can S&T better position itself for the current and anticipated shifts in the technology development market?
4.) Is there any concern that the USG will significantly reduce funding to basic and applied research and instead increase spending on accelerating/modifying existing technology to meet its national security needs?

Response Summary:

- Study projects going really well and see what the success is. Usually it's the skill of mobilizing the people who support the project. Focus on what individuals and organizations do well and turn them into SOPs and directives.
- Human factors are a big challenge for S&T. Collaboration could be improved to solve more problems.
- Long term trends continue regardless of administration and policies. Small companies get bought by big companies. Determine what matters.
- Current immigration policy can be a big challenge with partnerships with tech companies.
- Move the mindset to continental, not border to protect the infrastructure.
- Formulate a recommendation to make better use of OTAs. OAT and FAR are difficult to work with CORs and Office of General Counsel are risk adverse to work with partners. Build a culture on emergency contacts, fence off money to create a non-risk culture.
- More education and training. DHS could look at Virginia Governor McAuliffe's model where the state pays for cyber certification and the investment pays back within 2 years by new state tax on revues from filling vacant spots with certified workers.

4. LIGHTENING ROUND

Michel Kareis lead the final session of the day to facilitate discussion on

Response Summary:

- Collaboration and relationship building, in person meetings, creating awareness, and attending conferences. Use the 50 mile rule to keep costs low but the interaction going.
- Focus on education and DHS internships, DHS loan executive program.

- Innovation – hackathon, challenges, when we look at DHS problems there is an opportunity to bridge the way in the national security domain.
- Strategic thinking and planning is needed
- From a funding stand point, change the name in the budget to "management and training" instead of "travel and salary" to get the money.
- Spend more time with other components to know requirements in commercialization. It implies value that people are willing to buy it.
- Need to have networks with companies more than and arms reach away. What are DHS S&Ts needs? Funding efforts to get attention to what you need. Turn it into a lean and mean function
- Increase S&T mission space. Themes are engagement and leverage communities.

Comments from the Public: There are none at this time

5. **ADJOURN: Kareis** adjourned the meeting at 12:15 p.m.

Signed: Vincent Chan, HSSTAC Co-Chair **Date** April 10, 2017

Signed: John Sims, HSSTAC Co-Chair **Date** April 7, 2017

MEETING ATTENDEES:

Keith Bryant
Vincent Chan
Byron Collie
Philip Coyle
William Crowell (virtual)
James Decker
Daniel Dubno
Murray Farr
Michael Goldblatt
Marian Greenspan (virtual)
Yacov Haimes
James Hendler

Mark Maybury (virtual)
Annie McKee
Kathie Olsen
Gerry Parker
Harry Raduege
Gary Schenkel
Jim Schwartz
John Sims
Christina Williams
Ted Wilke

Others
Jason Ackleson
Brian Humphreys
David Olive
Jeff Booth
Denis Gusty
James Johnson
Daryl Kramer
Keith Holtermann
Michel Kareis
Susan Dixon Rhoades
Tod Companion
Matt Sarlouis
Shari Myers
Barbara McIntyre
Gretchen Cullenberg
John Copenhaver
Sally Harris (Virtual)
Velma Deleveaux
Mina (Aminah) Knight
David Price
Mark Protacio

NOTE: All meeting materials are posted at http://www.dhs.gov/st-hsstac. No handouts were distributed during the meeting.