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

November 3-4, 2016
Committee Meeting
Location: 1120 Vermont Ave., NW, Washington, D.C. 20005
Washington, D.C. 20005
Minutes

Summary: About 65 people attended the meeting (please see list below). A recording of the meeting sessions can be found at:
Day 1 Part 2: **https://share.dhs.gov/p9nqi1vdu8s/**
Day 2 part 1: https://share.dhs.gov/p24kdwh3br2/
Day 2 part 2: https://share.dhs.gov/p1afpfvqy27/

Day One (*Thursday November 3*):

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 to the first HSSTAC meeting of Fiscal Year 2017. The meeting is being held pursuant to the October 18th Federal Register Notice. She provided an overview of the agenda and notification that the meeting was public and being recorded. The HSSTAC members introduced themselves. .

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 September meeting. The commercialization sub-committee is trying to determine what public and private best practices can be brought to bear on the problem of turning research into commercialization efforts, tech transfers, transitions and additional funding for investments for the Homeland Security Enterprise and DHS customers. The subcommittee is continuing to work on understanding the commercialization challenges. The outline of the report has been completed on schedule.

Two asks for the committee. The first is that the committee takes time to review the report and give feedback when the draft report is completed. The second ask is the subcommittee is looking for additional members who have specific expertise with the DHS customer base. We would like to develop case studies for the report that shine light on how we can do more effective commercialization with all of the challenges involved.

There is a need for a market analysis business model, clearing if we can adapt existing products through minor changes is going to help companies be more financially successful with products. Some of these are very narrowly defined, very expensive investments. So the subcommittee is looking at it to make recommendations that will help companies be successful, help S&T assess whether they would be successful, and to facilitate opportunities. The subcommittee has heard of some of the challenges involved with bringing these things to market and getting them in the hands of the components and DHS user-base. Challenges include products coming late to the market, companies going under trying to fulfill contracts. The subcommittee wants to make recommendations to fix these problems. You fund an investment and deal with the success rate coming out of the pipeline. How can that be improved? The subcommittee is interested in needs or markets that are not being met the subcommittee does recognize that there is a policy and requirements disconnect. We would like, at least from and S&T perspective, to address that incentive. What we would recommend is that it get involved with standard development. Maybe there is need to do some research in policy. We're definitely doing some research in requirements and requirement gathering, and vetting.

Chief Keith Bryant, Chair, Subcommittee on Social Media Working Group provided an update on the subcommittee since September. There is a draft 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 report includes case studies of exercises at all levels including federal, state and local. The subcommittee would like to have the committee review and provide feedback on the report. This subcommittee is going to be developed into a FACA committee in order to address more of the issues publically. Denis Gusty from DHS will be managing the new FACA committee.

Dr. Vincent Chan, Co-Chair, Subcommittee on Internet of Things Smart Cities reviewed the original charter and objectives for the subcommittee. The charge is to provide a larger representation on a the following things: what does a smart city look like, two-fold variances one is for certain and one is more difficult to think about. What will the technology be in 5, 7, 10, timeframe so that DHS S&T can be prepared for it? The topic of the Internet of Things Smart Cities will be discussed in more depth on day two of the meeting at 9:15 a.m.

Meeting Open for Questions or Comments from the public: None at this time

3. THE QUADRENNIAL HOMELAND SECURITY REVIEW UPDATE

Dr. Susan Monarez, DHS, Deputy Assistant Secretary, Office of Policy, Strategy, Planning, Analysis and Risk presenting updates on the QHSR and laid out the landscape of activities that they have been engaged in since the last time we met with you. Monarez asked members to assess and make recommendations to the 2018 version of the QHSR in order to make the document more actionable before the December 31st, 2017 deadline. In the last discussion, we had outlined a series of activities. We called them foundational studies. They were to be completed during this administration; so between now and January of 2017. The goal was to be able to identify in a clinically agnostic way, what were the issues in the external environment that DHS finds itself in and that we will continue to find ourselves in over the next four years. In that context how do we define that in terms of risk, probability and the consequences associated with those various threat hazards that have been identified in the external environment? What is DHS chronically doing to mitigate that risk associated with the priority threats? This will be discussed in more depth later in the presentation. A final foundational document will be made public in a few weeks. This document will be used to communicate with our larger Homeland Security Enterprise and stakeholders. There will also be a DHS Strategic Plan that will be issued as a companion document to the QHSR. This iteration of the DHS Strategic Plan will identify goals, objectives, milestones and outcomes by which our business partners within the department, our partners in the White House and our partners on Capitol Hill will all be able to say well you identified what is important, have you accomplished what you said and we think is important. It's the QHSR and the Strategic Plan that will allow us to move forward.

Jason Ackleson, DHS, Director of Strategy, Office of Strategy, Plans, Analysis and Risk, presented the 2016 Homeland Security Trends Review (HSTR). The key purpose of this product is to analyze trends that will impact DHS over the next four years. There is also have a section later in the report that talks about the 20 year trends.

Ackleson provided an overview of the threats and opportunities for improvement in each of the five mission areas identified in the 2010 QHSR. The HSTR will inform DHS senior leaders by providing insight into current trends affecting homeland security and provide context for selecting QHSR 2018 study topics the five missions of the QHSR and asking feedback from the members. The five missions are as follows:

1. Prevent terrorism and enhance security
2. Secure and manage our borders
3. Enforce and administer our immigration laws
4. Safeguard and secure cyberspace
5. Strengthen national preparedness and resiliency

We derive our strategies and our approach from that larger structure that the White House sets out. We are engaged in interagency thinking, preparing to give way to talk about these issues and think about ways in which efforts can be coordinated. So these things do work hand-in-hand. We do what we can to do an interagency engagement, professional purposes in this report we focus on the DHS (lane) because we can't cover the entire government approach. But it is all part of a holistic picture there is an examination of adversarial intent from that point of view of how the adversary may attempt to view this in a particular way. So that is taken care of in the intelligence community perspective.

4. SCIENCE ADVISORY GUIDE FOR EMERGENCIES (SAGE) UPDATE

Joe Anello, SAGE - The most current update is we have 17 nominees from the HSSTAC for the guide and I want to thank everybody for doing that. It's been very valuable to us. Please continue to send nominees to the same S & T (SAGE) email address or you can send them to me personally. We refresh and update the guide every six months to make sure that SAGE advisors are still at the same phone numbers at the same organizations, they still have the same expertise.

Meeting Open for Questions and Comments from the public: None at this time.

5. UNDERSECRETARY SITUATIONAL UPDATES

Dr. Reginald Brothers, DHS, Under Secretary, Science and Technology Directorate (S&T). Dr. Brothers began by thanking the committee for their work and participation. He went on to highlight S&T accomplishments and identify where he thinks the organization needs to go. Morale was a big issue in my confirmation hearings and has been an issue with S&T. I've done a lot of walking around and talking to people to figure out the real issues. I found a lot of decisions were made without a lot of explanation. An employee council was established to identify root causes and address transparency and communication issues. Our employee satisfaction scores have significantly increased. The homeland security industrial base was an area that needed more focus. Companies had trouble engaging with S&T and knowing what problems we needed to solve. We started the Silicon Valley Program in an effort to engage with the tech industry startups and have provided seed money for innovation We are expanding our reach and identifying how to solve major problems. To expand this idea there was a focus on the Internet of Things (IoT). Specifically, resiliency in a Smart City and securing and recovering from a natural or man-made disaster. For example, one of our early pilots had to do with resilience and early warnings through officials for flooding in the Lower Colorado River Authority which covers a large segment of Texas. As far as our portfolio goes, our mission is so broad and we have 7 Component agencies to support that we had to design a way to determine what vector to work on. We developed a set of visionary goals, went out to social media and asked for comments. We developed a set of integrated products (IPTs) to address major problems that cut across the entire DHS enterprise. The next step is to prioritize the IPTs and that is what Dewey Murdick will present next.

Dewey Murdick, DHS S&T, Deputy Chief Scientist & Chief Analytics Officer Over the last year and a half we have been starting to better look at the gaps from our partners and starting to figure out how to prioritize which gaps need our money and which mission threats are coming over the horizon that we should be investing in? And the last part is technical awareness to make sure we're harvesting the right technology coming over the horizon and we're leveraging the right community. Characterizing where we are today, we know our portfolio. We have a good sense of the gaps, and we're starting to get our hands around the threat landscape. The next step will be to optimize that. We are starting to work on is being able to appropriately estimate and brainstorm which threats are coming over the horizon that aren't phase threats. With the Centers of Excellence (COE's), there are two fundamental challenges: One, is now that we have the IPT's, we have to be able to better align the research that the COE's are doing with the IPT's, because right now it's not aligned. The second thing we have to do is figure out how to take that academic research which by necessity has to be put in peer review journal form, but then somehow get it out of that form and get it into a form so senior leadership here or at the White House can appreciate.

Meeting Open for Questions or Comments from the public:

Question from the public: Michael Spitz, SAIC, when you've got tactical mission needs and you've got an R&D development, how do you link between that two full spaces?
Murdick, Those technologies that map most strongly to being able to interfere with that mission are ones that a human can see. Those that are pulled and linked are not. So machine learning is our friend, in this case. We have human annotation and then we can start to, when we have a million different technologies coming over, we can be able to do that classification.

6. CONTINUED DISCUSSION ON THE QUADRENNIAL HOMELAND SECURITY REVIEW (QHSR)

Jason Ackleson, DHS, Director of Strategy, Office of Strategy, Plans, Analysis and Risk, presented the 2016 Homeland Security Trends Review (HSTR). He provided an overview of the threats and opportunities for improvement in each of the five mission areas identified in the 2010 QHSR. DHS Office of Policy will conduct a comprehensive literature review and Component subject matter expert elicitation to identify key drivers of change in the homeland security landscape. The HSTR will inform DHS senior leaders by providing insight into current trends affecting homeland security and provide context for selecting QHSR 2018 study topics the five Missions of the QHSR and asking feedback from the members. The five missions are as follows:

1. Prevent terrorism and enhance security
2. Secure and manage our borders
3. Enforce and administer our immigration laws
4. Safeguard and secure cyberspace
5. Strengthen national preparedness and resiliency

Feedback from the HSSTAC committee members included the following: look at trends, use different metrics, look at interdependencies, how effective is the architecture that is being used, look at factors you have available and data points, use matrix and critical infrastructures.

Stuart Evenhaugen, DHS, Senior Risk Analyst, Office of Strategy, Plans, Analysis and Risk spoke on the Homeland Security National Risk Characterization findings. The Homeland Security National Risk Characterization (HSNRC) will examine the key threats, hazards, and other factors that pose a substantial risk to homeland security or that could significantly affect DHS's pursuit of its stated missions and goals. DHS Office of Policy will work with DHS Components to leverage existing risk assessments across the mission areas, develop complementary risk assessments for areas not currently covered by DHS Components, integrate risk assessment results, as appropriate, and produce an overarching risk assessment that looks across natural and manmade hazards.

Meeting Open for Questions or Comments from the public: None at this time.

ADJOURN: Kareis adjourned the meeting at approximately 4:25p.m

Day Two (*November 4, 2016*)

1.RECONVENE AND OPENING

HSSTAC Designated Federal Officer, Michel Kareis welcomed the committee members at 9:00 a.m. and summarized the agenda for the day.

2. IOT/Smart Cities Discussion

Dr. Vincent Chan, HSSTAC Co-chair, is also the chair of the IOT/Smart Cities subcommittee under the HSSTAC. The charge of the subcommittee is to define and provide advice and recommendations on: 1) what will the Smart City of the future look like 2) what are the security challenges 3) how do we make it more resilient 4) how the government should compose new applications on top of the richness of the commercial IOT 5) what would be the add-on R&D necessary.

For example, a Cyber-attack doesn't have to come out of a single geographic spot. The whole architecture of the Internet of Things – where are the sensors, where the data is located and what's the database management. Is it going to be unstructured? Is it going to be relational database? How do you have sensors that goes to sleep and can be woken up on command and things like that. How do we have standards that facilitate this kind of data interchange? We want multiple sensors be a path for different things to do things. If they're not interoperable with no interface standard, we're going to have a very hard time. So what is the right way that DHS should play in this arena and the government?

- **What will the Smart City of the Future look like?**
  In the near term, 3 to 7 years, here are five items to consider 1. Smart Cities will have driverless cars in many of the major cities and infrastructure to support mixed traditional transportation. 2. There will be an increase in centralized control of utilities and some serviced including the use of satellites, cellular, fiber WAN and LAN for networking, standardized applications, centralized and distributed data repositories (e.g. fog). 3. There will be lower power protocols (new) and more energy harvesting. 4. In order to properly implement the Smart Cities of the future Standards are needed to support data interchange. There is a concern that propriety protocols may impede interoperability leading to having government regulators and agencies to be involved. 5. Data analytics

will be applied directly to sensed objects like traffic flow. Numbers four and five are most likely to have government involvement.

In the longer term, seven plus years, there are six items to consider: 1. Ubiquitous sensors and actuators. 2. Proliferation of networks to support data from the Internet of Things. 3. Widespread use of CCTV/sensors with built in biometric recognizers. 4. Integration and control systems to support decisions with quality information and efficient responsive city services. 5. New applications for businesses, government and citizens to access the IoT and data analytics recognizing outliers and potential compromises, etc. 6. IoT security and its applications to protect cyber-physical systems. Items four through six indicate likely government involvement.

- **What areas will the improved capabilities of the smart city affect?**
  National Security and emergency preparedness, crime prevention, first responders, transportation efficiencies and effectiveness, energy efficiencies and effectiveness, educational improvements, retail business efficiencies and effectiveness, and all aspects of the entertainment industry. There will likely be government involvement in the first five items.

- **What are the security challenges?**
  There are several near term challenges between now and seven years from now: 1. Control systems and applications must be secure but also provide easy access to IoT. 2. We must have secure network systems for IoT. 3. Most sensors and actuators are not likely to be secure due to power/computation constraints therefore creating the challenge to accommodate unsecure endpoints and secure the system. 4. Autonomous vehicle hardware and software security 5. Patching software and updating infrastructure for endpoints in IoT. 6. IoT security requires cooperation of multiple entities and organizations but can be impeded by IP and business profit issues. 7. Separation of security and authentication requirements for monitoring and action based channels. Action based channels require significantly more authentication and verification for the execution of control functions. Any IoT system which can potentially impact life safety should be considered a supervisory control and data acquisition (SCADA) and subject to certification. 8. IoT security or lack-of can affect the following: theft of intellectual property or strategic plans, physical criminal activity can be increased, financial fraud, reputational damage, business disruption, destruction of critical infrastructure, and can be a threat to health and safety. 9. IoT systems are likely to use cloud technologies for cost effectiveness which means organizations will have data storage at their physical presence and also potentially stored in locations outside of their control unless they plan for trusted, integrated solutions providers. 10. Different vendors may use separate and non-interoperable cloud provider, leading to a loss of interoperability. 11. IoT is really a SCADA/ICS (industrial control system) at large and poses the same risks and challenges such as: patching and upgrading (we have a chance to design in now as opposed to legacy SCADA systems). Security of codebases and development channels at vendors,

verification of patch veracity before implementation on the IoT device, reboot challenges, and vulnerability management. The supply chain challenge for trusted systems will expand for consumer and commercial vendors to develop code in less trusted locations. It is extremely likely that sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes. Very hardware oriented IoT implementations will likely face a similar End of Life, legacy and maintenance challenges that ICS and other embedded systems currently face. Modularity is the solution to allow for an easy upgrade of relevant hardware components.

What are the long term security challenges?
There are several long term, seven plus years, challenges to consider: 1. Compromised nodes and fraction of network infrastructure will be routine. A system must be planned for operation in the presence of compromised assets. 2. "Insider" attacks are a distinct possibility. There should be a way to sense, isolate, mitigate and operate through such attacks. 3. Preventing "normal accidents" and deliberate sabotage in complex composed IoT systems is a must. 4. Security in the dynamic changing IoT system must be maintained. 5. Cyber and physical security are increasingly interlinked. IoT can be used as an overlay for cyber-physical security applications but also can be used as a point of entry for attacks. 6. Data volumes and criticality of network connectivity are going to skyrocket with IoT. This poses questions for how devices function when connectivity is not available and device susceptibility to exploitation in this state. There needs to be a "fail safe" standard for devices. 7. IoT introduces massive vulnerability for electromagnetic disruption, either man-made (EMP, HERF etc.) or natural. Similar to the fail-safe situation, IoT devices require minimal essential functionality that is not dependent on connectivity etc. 8. Plans for disaster recovery and critical systems restoration must take into account distributed sensor networks and loss of communications with responders and devices.

- **How do we make it more resilient?**
  In order to make smart cities more resilient we need to consider several items: 1. Protecting critical assets against known and emerging threats across the ecosystem, perimeter defenses, vulnerability management, asset management, identity management, and data protection. 2. We will need to gain detective visibility and preemptive threat insight to detect both known and unknown adversarial activity by looking at threat intelligence, plus internal security monitoring, behavioral analytics, and risk analytics. 3. There will need to be an increase in strength and ability to recover when incidents occur through incidence response, fast, adaptive and automated responses to contain damages, looking at forensics, and crisis management and reconstitution of thin-line capabilities. 4. There needs to be a comprehensive security architecture and plan in place. 5. Information sharing and collaboration among agencies and departments is a must. 6. Red Team

exercise and certifications are vital for preparation. 7. There will need to be constant monitoring of IoT control systems and improvement on response to faults. 8. Create a new security paradigm and architecture construct that assumes compromised resources and insider proliferations but IoT still provide useable services. 9. Create an architecture for time-critical applications to react to and function through "black swan" events, e.g. zero-day attacks. Architectural resilience for disaster recovery is key. 10. Create an architecture to maintain control plane security, especially with SDN. 11. Possible use of satellites as thin-line, command and control and reconstitution, i.e. a heart-beat network. 12. We will need security research focused on dynamic (but bounded by M2M devices) environments. 13. New standards should be created to support interoperability at different timing and data volume scales. 14. New algorithms to support data fusion and validation/cross-checking of large number of measurements with unknown certainties, including machine learning interfaced with a corrective control system. 15. Application to improve cyber-physical systems security. 16. Develop control system theory where the internal states and feedback mechanisms of networks are intimately affected by inputs (traffic) 17. Develop cognitive networking where "network" senses current network conditions to improve resource management based on observables.

- **How would the government compose new applications on top of the richness of commercial IoT? What would be the add-on Research and Development necessary?**

  By looking at the Local 311 emergency management call system, for example, if the system was augmented to have broader regional and national centers to supplement existing citizen call-in mechanisms this would allow for other regions to help municipalities and states when they are hit with attacks on IoT infrastructure. It would also provide feedback for other disasters that affect a region like hurricanes, flooding, and oil-spills. 2. There needs to be increased government funding for R&D to improve the government related Smart City needs. 3. We need to foster architecture of interoperability between services, public works, and public safety for an enhanced quality of life. 4. There needs to be Common Operating Procedure (COP) developed to serve multiple users to include intelligence, dispatch of activities, data analytics, determination of distribution of resources and ability to connect and disconnect to the IoT Smart City Platform as necessary. 5. There needs to be an IoT security "add-on" encryption, especially to control systems to insure security of the system and detect problems in critical infrastructure. 6 IoT sensing will monitor various IoT systems to sense large-scale faults and correlate data among different IoT systems (e.g. atmospheric monitoring with electrical grid with seismic sensing for natural disasters). 7. There needs to be an application to add security of other systems. 8. Support the use of IoT, SDR, SDN, and cloud technology to connect multiple radio modality for emergency disaster relief.

- **What Actions should the government take?**

  The following items are recommendations that the government should consider: 1. Reach across multiple departments and agencies, including state and local government, to create an integrated approach and coordination to protect IoT Smart Cities. 2. The government must develop more focused and secure applications to ride the richness of the commercial IoT. 3. A critical government review must be undertaken of the value and need to connect various sensors, processing and storage, allowing for connectivity without an identified purpose only adds to the vulnerability of the network. 4. Government funding for R&D must be increased in order to improve the government-related Smart City needs. 5. Create a governance and operating model, identify policies and standards including interoperability. 6. Review and assess management processes and capabilities. 7. Create risk reporting on all threats. 8. Provide risk awareness and culture education. 9. It is extremely likely that sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes. 10. The government may need to look at common criterial like a certification process to develop trust in IoT, particularly for life and safety oriented applications similar to the ARINC 653 specification for avionics systems; use critical mass between localities, state, federal acquisitions to enforce standardization.

3. **Jeff Booth, S&T First Responder Group**
   Requesting input and review of draft Next Generation First Responder (NGFR) Quick Start Guide. The request is to review the draft NGFR Interface Control Document (ICD). The document will support global & U.S. market first responder requirements & gaps, IoT first responder sensors, applied R&D for smart/safe Cities, responder interoperable sensors & open standards. Is there such a thing as virtual network system for IoT? Is an IoT network even securable? There are lots of people in the security business who say it is. We use strong crypto graphics. Strong crypto graphics assume that the user is trustworthy. We have to rethink network security. The power grid, using SCADA system, is not going to change. Its standard everywhere. It’s embedded in devices. First Responders definitely have a need for these items... They need it for situation awareness and responsive actions.

Jeff Booth, First Responder Group
Booth covered the Forum’s Global Market Survey 2014 and the First Responder market overall expenditures We think that the current R&D budget for smart cities is not sufficient to even deal with the specific things that the government should do. Some of those things are, for example, interoperable architecture between different surfaces. A common operating picture to be generated so the city manager can see what’s going on and actually react accordingly. US Public Safety Community, Technology Adaptation:

Community Profile, FRG’s Solution Development Process, FRG Membership, Most Critical Capabilities, Smart City and IOT Flood Sensor R&D.

HSSTAC Member Comments: There are things we can do with the processors to help with this problem. There are ways of separating executable code from data. There are trusted execution blocks that are now part of modern processors. And there are – technologies such as secure enclaves that will help them. To protect against outside attacks you need monitoring, including monitoring your own people.

In 2015, in collaboration with other agencies, the White House announced a program in smart connected cities. In 2016, they held a big initiative creating test beds for the internet of things, applications, developing a new National Science Foundation program on connected and smart cities. NIST and the Department of Energy are also involved.

IoT First Responder: Sensors & Communications Open Standards Interoperability On the list of the aspects of smart cities. Note the absence of anything related to healthcare. And healthcare is a big part: early warning through wearable sensors.

IoT for First Responders: To-Be Architecture First responders are facing challenges never envisioned a decade ago. As part of homeland security science and technology director to our next generation of first responder programs, is looking at new technologies, the art of the practical. As more data is available, analytics will serve as key information and presented in a way that is easy to digest on the way to a scene or during an emergency incident.

Arun Vemury, DHS Science and Technology, the S&T, FRG organization traditionally works directly with first responder groups in cities but when we start talking about smart cities, the question is now how we need to be talking to urban planners, we need to be talking to city managers, we need to be talking to city hall. How can we contribute our knowledge, not only our expertise, but our knowledge, and competencies to inform smart cities or the development and emergence of smart cities over time? First responders are a use case or an application that cities already understand and know.
What we've learned so far from data analytics and other resources and share them with cities to help accelerate the learning curve, right, to bend that learning curve so that they're not starting from scratch. . One is you want to have some standardization and simple things that you give as tools to the cities so that they can react in a way that they have to. On the other hand, you'd want to avoid a monoculture. The fact that each city is going to go off and do its own thing, regardless of what other cities are going to do could be a very good thing.

Comment from HSSTAC Member: Diversity when it comes to communication protocols, is not good. That's what breaks browsers and makes systems not interoperate.

Questions to Consider: What are the security challenges? Near term: now -7 years, how do we make it more resilient?

Meeting Open for Questions or Comments from the public: None at this time

ADJOURN: Kareis adjourned the meeting at 3:00 p.m.

February 2, 2017

Signed: Vincent Chan, HSSTAC Co-Chair **Date**

John A. Sims

February 2, 2017

Signed: John Sims, HSSTAC Co-Chair **Date**

MEETING ATTENDEES:

Keith Bryant
Vincent Chan
Byron Collie
Philip Coyle
James Decker
Daniel Dubno
Murray Farr
Marian Greenspan
Yacov Haimes
Eric Haseltine
James Hendler
Annie McKee
Kathie Olsen
Gerry Parker
Gary Schenkel
James Schwartz
John Sims
Brian Toohey
David Whelan
Roy Wiggins
Ted Wilke

Others

Michelle Atchison
Reed Skaggs
Jason Ackleson
Brian Humphreys
David Olive
William Ruch
Cynthia Dion-Schwartz
Brandon Barnett
Michael Spitz
Daniel Marasco
Jeff Booth
Mitch Erickson
Snyder Justin
Evrim Bunn
Arun Vemury
Denis Gusty
Norman Speicher
Joe Anello
James Johnson
D. Kramer
Keith Holterman
Michel Kareis
Susan Dixon Rhoades
Tod Companion
Joseph Martin
Matt Sarlouis
Shari Myers
Barbara McIntyre
Gretchen Cullenberg

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