Surface Transportation Security Advisory Committee (STSAC)

Meeting Minutes

October 24, 2019

Meeting Summary

The second meeting of the Surface Transportation Security Advisory Committee (STSAC) was held at the offices of the American Public Transportation Association (APTA) in Washington, D.C.

Transportation Security Administration (TSA) Leadership and the newly elected STSAC Chair Thomas Farmer and Vice-Chair Polly Hanson addressed the Committee. Presentations were provided by TSA personnel on TSA Restructuring and Organizational Changes, Surface Intelligence Information Sharing Cell (SISC), Insider Threat, Section 1964 of the *TSA Modernization Act*, Surface Transportation Security Technologies, Sensitive Security Information (SSI), and the STSAC Homeland Security Information Network–Critical Infrastructure (HSN-CI) Portal. Committee discussions focused on the topics of Cybersecurity and STSAC Priorities.

Meeting Comes to Order

STSAC Designated Federal Official (DFO) Henry Budhram, Jr. welcomed the Committee members and called the meeting to order at 10:30 a.m.

Safety Briefing

APTA Director of Security, Risk, and Emergency Management Polly Hanson provided a building safety briefing.

Opening Remarks

STSAC Executive Sponsor Victoria Newhouse, Mr. Farmer, and Ms. Hanson delivered opening remarks welcoming the STSAC members to the meeting.

Ms. Newhouse recognized the voting members for assembling privately to organize and discuss priorities prior to the committee meeting. She was extremely honored to participate on the Committee, pleased with the selections for Chair and Vice-Chair, and looked forward to the Committee's new ideas. Special thanks were given to Executive Assistant Administrator (EAA) for Operations Support Stacey Fitzmaurice, Deputy Executive Assistant Administrator (DEAA) for Operations Support Aaron Roth, Assistant Administrator (AA) for Surface Operations Sonya Proctor, Acting Executive Director of the Surface Policy Division for Policy, Plans, and Engagement (PPE) Scott Gorton, and DFO Henry Budhram. Ms. Newhouse looked forward to the afternoon visit of David Pekoske who was serving as the Senior Official Performing the

Duties of the Deputy Secretary of the Department of Homeland Security (DHS) as well as in his position as the Administrator of TSA.

Mr. Farmer recognized the diverse backgrounds of the Committee members and thanked them for volunteering their expertise. Mr. Farmer noted that there will be many opportunities for the Committee to drive positive change as part of the collaborative solution to the log-jam in government. One such example was focusing more attention and resources on surface transportation security than in the past to stay ahead of and continue to thwart the physical and cyber threats.

Ms. Hanson welcomed everyone on her behalf and that of APTA Leadership.

TSA Restructuring and Organizational Changes

TSA Deputy Assistant Administrator (DAA) for Policy, Plans, and Engagement (PPE) Victoria Newhouse spoke briefly about some of the realignment and organizational changes that will affect surface transportation. DAA Newhouse anticipates that an Executive Director for the Surface Policy Division will be named in the near future and there will be some realignment of functions within Surface Policy. Ms. Newhouse then introduced Assistant Administrator (AA) for Surface Operations Sonya Proctor to provide an overview of developments within Surface Operations that will enhance the scope of TSA's national, local, and regional engagements.

AA Proctor thanked the meeting participants, noting that everyone had some relationship to surface transportation. What was known as the Surface Division has become two organizational elements—policy and operations. Surface Operations is now a unit under Security Operations and the Surface Policy Division is part of PPE. Ms. Proctor reassured the Committee that even with this organizational restructuring, surface transportation stakeholders will continue, in large part, to engage with the same TSA personnel they have worked with in the past.

Surface Operations will utilize the 260 Surface Transportation Inspectors (TSIs) working out of 47 field offices to deliver services in the field. The TSIs will provide surface transportation security policy implementation and execution, inspect for regulatory compliance, and assess the implementation of security guidelines for the mass transit and highway modes in the form of Baseline Assessment for Security Enhancement (BASE) evaluations. Surface Operations will also offer training and exercise delivery through the First Observer Plus™, Exercise Information System (EXIS), and the Intermodal Security Training Exercise Program (ISTEP). The new structure allows for the potential to expand and deliver a greater variety of services by leveraging more people to do tasks that the headquarters staff had performed in the past.

Ms. Newhouse received many questions specific to organizational alignment and how activities such as intelligence information sharing, policy, and training would be supported under the new structure. She reiterated that Administrator Pekoske has adamantly emphasized the necessity of creating a "one-stop shop." Under the new structure, TSA Surface Operations staff will be available around the country for assisting surface operators with information sharing, security planning, training, and exercises. The Surface Operations staff in the field will coordinate with staff at headquarters with a goal of making additional resources available in the field. The PPE

Industry Engagement Managers will remain the primary points of contact for national level engagement with trade associations and industry working groups.

Mr. Farmer addressed the Committee and noted that the new organization of TSA for surface transportation including field inspectors is within the scope of the Committee's ability to provide recommendations to support effective resource allocation decisions. Recognizing that TSA surface inspectors will be working on compliance and training delivery, Mr. Farmer inquired about tasks and how they would be split locally—who would do, as an example, regulatory oversight and who would do training. Ms. Proctor explained that surface inspectors would be working in both regulatory and voluntary environments as they have been for a number of years. AA Proctor acknowledged that the approaches taken to regulatory compliance and voluntary assessments and reviews are different; and because there is a base of experience doing both with the same workforce, she is confident that the personnel in the field will be able to balance these varied assignments.

Ms. Newhouse described TSA efforts to ensure consistent interpretation for inspectors determining what the regulations really mean. The TSA PPE Policy Coordination Branch (PCB) has initiated a pilot program focused on ensuring consistent policy interpretation in the aviation domain. The PCB repository enables TSA to communicate about TSA policies more consistently and with greater understanding about the intention of the policy. This initiative will eventually include the surface transportation domain.

Committee members asked about intelligence being delivered to the field as a result of the organizational change and if there would be any impacts to the Field Intelligence Officer program. Executive Director for TSA Intelligence and Analysis John Beattie responded that Field Intelligence Officers (FIOs) are staying in their current locations and will be expanding their engagement with stakeholders in the field.

TSA I&A Surface Intelligence–Information Sharing Cell (SISC)

TSA Executive Director of Intelligence for Intelligence and Analysis (I&A) John Beattie spoke to the Committee on TSA information-sharing initiatives. Mr. Beattie oversees the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC) and the SISC. TSA currently provides products to industry stakeholders through the PPE Industry Engagement Managers, direct email, and postings to shared information portals. I&A is now working to implement a more formalized method of product delivery and engagement that will make the intelligence information-sharing process more efficient, sustainable, and repeatable. Future goals include leveraging the Committee to help TSA develop a timely way forward for information sharing by building forums for multi-modal information sharing based on the Administrator's Intent. Mr. Beattie recognized the importance of improving two-way information sharing between government and industry to ensure both parties get the right inputs for the right outcomes collectively delivered.

The SISC is built on the ADIAC model consisting of three major business lines:

1. Knowledge Management—identifying available information and putting it where industry and government can each see it

2. Cataloging Requests for Information—involving different requirements depending on stakeholders and their industry, and methods for identifying such

3. Crosswalk—developing the best posture to answer information requests

The SISC will focus on collecting information, cataloging requirements, and then sharing information back with government and industry partners. SISC will work with existing government and private industry surface transportation organizations, structures, and processes to facilitate the flow of two-way intelligence and security information sharing.

Mr. Beattie looks forward to working with the STSAC to develop the SISC and the best way to enhance two-way information sharing between government and industry. Mr. Farmer thanked Mr. Beattie for the presentation. Mr. Farmer referenced the Rail Intelligence Working Group (RIWG) that has formed a unique partnership between Associations and government organizations and now serves as a way for the government to provide information to industry without going through a long review and clearance process. The RIWG quickly produces actionable information and shares it with industry. Mr. Farmer understood the need to develop a defined method for sharing to increase the profile of sharable information; however, he was unclear about what the SISC would do and how it would add value. He believed the most important consideration is fast turnaround when trying to prevent an attack. Mr. Beattie added that SISC needs to determine the most appropriate forum to use—email, phone call, and so forth—and that the ADIAC model could provide some insight.

Insider Threat

DFO to the Aviation Security Advisory Committee (ASAC) Subcommittee on Insider Threat Dan McCann and TSA Strategy, Policy Coordination, and Innovation (SP&I) Transportation Security Specialist Dean Walter delivered the presentation on Insider Threat. Mr. McCann provided insight into the history of the working group that the ASAC established in 2015, succeeded in 2018 by a joint industry-government standing subcommittee, to address the TSA Administrator's concerns with the insider threat. Areas of focus have included vulnerabilities exposed by a gun smuggling ring from Atlanta Airport to La Guardia Airport and the Seattle stolen-aircraft incident. Most recently, the ASAC developed an Insider Threat Report containing recommendations for TSA. The recommendations have been accepted by the Administrator, and TSA and the ASAC are now working toward implementation.

Mr. Walter discussed the development of an Insider Threat Roadmap that will serve as the sector's strategy for countering insider risk. This document will align with and leverage the ASAC Insider Threat Report and cover all modes of transportation. Preliminary outreach has been conducted with public transportation stakeholders through the auspices of APTA. TSA will coordinate the strategy with the STSAC and ASAC before issuance. Mr. Walter recognized that much of the focus has been on aviation and more attention needs to be placed on the whole "ecosystem" of transportation security. The timeline is to have a draft document ready for review in December 2019 with final issuance in early 2020.

TSA Surface Transportation Security Assessment and Risk-Based Strategy (*TSA Modernization Act* Section 1964)

TSA Executive Director of Enterprise Performance & Risk for Strategy, Policy Coordination, and Innovation (SP&I) Jerry Booker and Transportation Sector Security Risk Assessment (TSSRA) Project Manager Keon Baxter presented the development process of the security assessment required by Section 1964(b) of the *TSA Modernization Act*, *Surface Transportation Security Assessment and Implementation of Risk-Based Strategy*. The scope of Section 1964(b) requires an assessment of the vulnerabilities of and risks to surface transportation systems.

Now that the Surface Transportation Security Assessment is complete, Mr. Booker looks forward to the Committee helping with the cross-cutting, risk-based surface transportation security strategy document due next year. The goal is to have the final draft prepared by the end of December, 2019. Per the legislative mandate, the document is due to Congress in April 2020.

Committee members noted that there is a disconnect between what information is provided by the subject-matter experts (SMEs) and what is actually happening. A key concern is the failure, in engagement with various constituencies, of TSA officials to cite the substantial achievements and progress made in surface transportation security—as a demonstration of the public-private partnership in action. There was discussion on the importance of including criminal activity and how that could translate into possibilities for terrorist attacks. Committee member Denise Krepp recommended that criminal activity be considered and incorporated into the assessment and final document. Mr. Booker indicated this may be problematic because the frequency of criminal activity is very different from terrorism activity, both foreign and domestic. Funding streams and outcomes also differ between criminal and terrorist activity. This does not mean that the criminal activity issue should not be looked at—it just needs to be looked at differently.

A Committee member noted that the strategy document may be redundant to other existing documents such as the National Strategy for Transportation Security (NSTS). Mr. Gorton recognized the redundancy. However, TSA is obligated to do what Congress directs and the strategy is a requirement from the *TSA Modernization Act* (Section 1964). The NSTS is mandated by the 9/11 Act. The Surface Transportation Security Assessment and Implementation of Risk-Based Strategy are requirements of Section 1964 and will have more focus on the process of assessing risk and identifying operational objectives. The objectives in the Surface Strategy will be complimentary and not contradictory to the NSTS.

Cybersecurity—Intelligence and Information Sharing

Mr. Farmer and Mr. Scott Gorton led the discussion. They recommended that the Committee work on identifying possible approaches to quickly share potential cybersecurity attack indicators and a mechanism to broadly share this information across the surface enterprise.

Mr. Gorton noted that TSA is aware of the productive information sharing occurring within the individual modes and there is a potential for additional benefit by sharing cyber-related information across the surface modes. The challenge is identifying a process and rules of governance that will afford the appropriate protection to the reporting party and allow for the

rapid processing and dissemination of information that can be of value in defending against future attacks.

For example, information could come from operators, go through a trusted third party like an ISAC to be anonymized and categorized, and then be sent to TSA for distribution across the surface enterprise. The Committee's input and recommendations on how a "cyberattack alert" network might function will be vital to a successful standup.

Mr. Gorton recognized that there are always questions about how TSA and the industry know if we are collectively doing a good job or making improvements in security. While there are metrics associated with objectives identified in the National Strategy for Transportation Security, these performance measures do not fully represent the scope and level of effort of transportation operators are providing for their operations. Performance measures should be able to tell us how we know things are more secure—although, sometimes there are problems in that a lot of performance measurements are outputs and not outcomes. TSA would like to obtain the data necessary to answer the question—how do we know if we are doing better? The Committee is a good venue to provide informed input as to how we can collectively do a better job in identifying data that more fully tells the story. TSA will be asking the Committee to recommend performance measurements that work, that both industry and government can live with, and that are practicable, doable, and effective in the end-state.

TSA Surface Transportation Security Technologies

TSA Executive Director of Intermodal Division (IMD) for Requirements and Capabilities Analysis (RCA) Robert Pryor provided an overview of security technologies that TSA is currently testing in operational environments. His office focuses on industry as their primary client, not the government.

Mr. Pryor noted that many of the Committee members are familiar with the testing methodology that his office uses and that his office has turned into the "Consumer Reports" for transportation security technologies. IMD does not buy anything—rather IMD assesses what is available in the marketplace. A technology must make it through rigorous lab testing using realistic threat scenarios to determine how well a piece of equipment or system will perform in the field. IMD collaborates with the Research & Development Working Group (RDWG) each year to identify capability gaps that become the subject of research and testing. Mr. Pryor reiterated a need for testbed partners as he wants to expand the number of testbeds geographically.

Mr. Pryor's group also has responsibility for Unmanned Aerial System (UAS) detection research. For this, IMD focuses mostly on airport perimeters and adjacent areas and is currently determining potential testbed sites including one for surface transportation. Mr. Pryor noted that detecting and defeating unauthorized Unmanned Aircraft Systems (UAS) operations is complicated because of the need to coordinate with the Federal Aviation Administration (FAA) and other agencies to determine authorities.

Ms. Hanson recalled how she worked with Mr. Pryor during her time at Amtrak. She sees his group as a valuable resource for the technology they needed and ensuring that it performed as

promised. She encouraged Committee members to get in touch with him to find out more and participate.

Administrator Remarks

Administrator Pekoske thanked everyone for their work and commitment to the Committee and noted his recent travels with AA Proctor talking with industry at forums and discussions.

He recognized the Committee's efforts to set up priorities going forward and asked the Committee to look at cybersecurity and how it can be emphasized from different dimensions. It is important to understand the cybersecurity threat to the extent that it really needs to be understood. Cyber threats are very real and time is not on our side—we need to move quickly. Government works at a different speed from industry—industry needs to keep the government on task. Administrator Pekoske is trying to redefine the speed of government because the security business cannot revolve around methodical processes in a hierarchical system to make decisions.

Administrator Pekoske emphasized insider threat as another priority. He recommends the Committee look at the ASAC recommendations and determine how they might be modified or adjusted to meet surface transportation security needs.

Administrator Pekoske stressed the need to move forward on the regulations mandated by the 9/11 Act. He asked the Committee to look at the concept of "structured oversight" and how we can narratively go beyond what we are saying and how we are labelling things to how we move beyond voluntary guidelines. He is concerned about the misperception that voluntary means there is no structure and no oversight. While TSA successfully works collaboratively with industry on voluntary security initiatives, TSA has regulatory authority that can be exercised in short order to address threats. So, what is the middle ground between regulations and staying within a voluntary collaborative environment? Administrator Pekoske asked the Committee to reflect on what "structured oversight" might look like and provide recommendations as to how TSA and the industry can better document the amount of security preparedness that is taking place across the surface domain.

Mr. Farmer emphasized the need for subcommittees to address the collective challenge of cybersecurity and insider threats. He agreed with Administrator Pekoske on the issue of "structured oversight." This term could also be called "public-private partnerships in action" for example—Security Action items (SAIs) and the guidelines necessary to move people and products to their destinations. Whether we use the term "public private partnership in action" or "structured oversight", the Committee will focus on ways we can better tell the story of surface transportation security.

Administrator Pekoske concurred with Chair Farmer. He agreed 100% that some of our language may not fully represent what is actually going on—actual reality—and more work needs to be done to further define the public-private partnership that will tell a story of industry and government closely knitted together. Administrator Pekoske sees value in the Committee because it can talk about something consistently when interacting with their own stakeholders

through their organizations or on Capitol Hill. The STSAC has the opportunity to better define what a public/private partnership looks like and how it can be used to meet the expectations of the government and industry. Administrator Pekoske reiterated his thanks to the Chair and Vice-Chair for stepping into the leadership roles. He also thanked APTA for the great conference space. He highlighted the work done by EAA Fitzmaurice, AA Proctor, and AED Gorton to help move these efforts forward.

STSAC Priorities and Open Discussion

Mr. Farmer noted Administrator Pekoske made good points, especially when it came to working in concert—both government and industry want to succeed with transportation security and ensuring movement of goods and people. Each group is invested in the other's success and how to make it better. Mr. Farmer stressed the importance of trying to achieve consistency because he has seen so much inconsistency. Industry and government have tried a modal approach. There are unique aspects of each mode, yet these aspects are not so unique that other modes cannot benefit from the caliber of work being done in one location. The recommendation was to look at all modes together to better understand the threats and objectives for surface transportation security.

Other recommendations included utilizing cross-border information sharing taking into account multiple modes. Mr. Farmer has found lots of commonalities in threats that each mode faces such as terrorism and environmental activism, and he believed we could learn from other countries including the British as to how they addressed these threats.

Mr. Farmer cited the importance of ensuring consistency across different modal entities that might begin with compiling aspects of effective practices to use as a good comparative resource. While different effective modal practices may not apply to all modes in a direct sense, it is likely something about them could be applicable, particularly with cybersecurity. Mr. Farmer again asked, "How do we ensure we are doing more to share information across the board?" The word "threat" comes up in various ways—terrorism threat, crime threat, disruptions to operations that can damage infrastructure. If an operator understands what the adversary looks at, it can present a security posture in a way to give terrorists pause. Different proactive activities on the operator's part cause the adversary to wonder.

Mr. Farmer then returned to cybersecurity as another area of emphasis—also one of Administrator Pekoske's recommendations. He recommended tackling this by first taking already available information and using it better. He urged the Committee members not to lament the information they do not have—rather use what they do have as thoroughly as possible. The indicators and some of the technical information are available. The next step is to do a better job of sharing that knowledge. Many information technology systems are the same; consequently, the adversary focuses on that as opposed to an individual mode. Sharing in a non-attributable way will have great benefit. From a risk-management perspective, this helps narrow the risk profile.

Mr. Farmer suggested that another focus area that may prove helpful is risk assessment or adapting approaches in a way that makes sense. There is a commonality of threats in terrorism

and destructive activism, and there is a great deal we can learn from what internal communities are doing. There is a difference between free speech and those who cause damage and destruction. Work needs to be done to ensure greater consistency across the modes. Information sharing is a two-way street—it is important to look at what industry needs from government and at what government needs from industry.

Mr. Farmer suggested looking at supply-chain risk—such as where materials come from—and then leveraging information on criminal activity, particularly if it lends itself naturally to something a terrorist can use for a more nefarious intent.

The SISC can create a network in a true sense that will prove tremendously successful if it avoids bureaucratic hurdles. The non-attributable cyber-concept would also serve as a good model. Challenges occur more in logistics because of the necessity of ensuring people pass through appropriate vetting. Mr. Farmer saw the concept of a SISC information–sharing network that will convey and disseminate information on threats as a good place to start.

Mr. Farmer returned to the insider threat issue. He found that different credentials used—from cards to driver's licenses—are a problem and may present an opportunity for economies of scale for proper vetting. No regulation is necessary for this. A pilot test could see what works first and then put a performance-based system in place. Mr. Farmer cited another area raised by Committee members—cargo/supply chain security, particularly with HAZMAT and food security. Examining this presents an opportunity to better understand the system and ways to protect it.

Mr. Farmer stated that emergency preparedness means that an agency plans properly for manmade and natural disaster. He highlighted the I-STEP program where regional exercises cover realistic scenarios—but the gap is "What is left behind?" after the exercise. The need to create localized regional information sharing remains. Exercises provide the chance to learn the capabilities available in the area. A consistent approach for emergency preparedness and bringing resources to bear from long distances would definitely help responders, as would normalizing approaches and getting the clearance for people to come into the area to help.

Finally, Mr. Farmer added that another area for subcommittee focus is to look at technologies and determine what operators should obtain and why. We are all working with limited resources and want to go to a reliable source to determine the performance parameters before purchasing equipment.

He summed up his remarks by recalling the thorough discussions and the need for all members of the group to bring to bear their expertise.

Further discussion among Committee members included:

- Leveraging information from criminal activity which may be indicative of an opportunity or area vulnerable to a terrorist attempt
- The need to be concerned about foreign manufacturers developing products that may try to disrupt transportation networks, physical and cyber—such as access by foreign intelligence

services to information obtained by drones or surveilled by camera systems in passenger rail cars manufactured by state-owned or supported enterprises

- A need for clarity on what the Committee is supposed to be delivering to ensure what is being developed will not sit on a shelf collecting dust

- A recommendation to educate Congress, to better understand the redundancy of reports, and the value of focusing on implementation and the analysis of the information

- A recommendation for having greater participation in the grants process

Mr. Farmer noted the DHS assessment in recurring National Terrorism Advisory System (NTAS) Bulletins over the past nearly 3 years that we are facing the most serious threats since 9/11 while, at the same time, there is a drop in federal funding. In terms of assessing risk and determining how to mitigate risk, we need to align resources.

Ms. Newhouse stated that the STSAC should advise TSA leadership on "What can the government do in collaboration with their security partners?" TSA looks for those kinds of outcomes and wants to capture that in the right tasking letters, putting the Committee in the best position to deliver on their tasks. She pointed to grants, another area that can hit everyone and, while it is always nice to ask for more money, the two key areas right now come from insider threat and cyber. She promised a formal letter would come out describing these focus areas.

Mr. Gorton noted that the *TSA Modernization Act*, Section 1931(d) required a report on the carriage of firearms in aviation and surface transportation. Many regulations exist for the aviation side; however, it is less clear as to what rules apply when it comes to public transportation. The Act requires consultation with both STSAC and ASAC and TSA will issue a formal letter in order to receive information from the Committee about the carriage of firearms by individual persons riding on a surface conveyance.

Administrative Discussion

TSA Sensitive Security Information (SSI) Brief

TSA SSI Program Analyst Deirdre O'Sullivan provided the Committee with an overview of the SSI Federal Regulation (49 CFR Part 1520) and the importance of protecting SSI for surface transportation security. Everything that committee members may need to know about SSI is in a four-page regulation advising what it is, how to protect it, destroy it, share it, and what happens if you misuse it. Unlike many other federal agencies, the SSI Federal Regulation requires that TSA mark sensitive documents as SSI rather than For Official Use Only (FOUO). To be considered SSI, the information must fall into one of the categories protected by the regulation. FOUO does not provide protection in a court proceeding and may be released.

To access SSI, the SSI Federal Regulation dictates that a person must be a "covered person" with a "need to know." "Covered persons" must work in the transportation industry such as a railroad, pipeline company, port authority, or work for the federal or state government. "Need to know" means that this "covered person" also must access the SSI in order to accomplish their official duties. Any questions for the TSA SSI Program may be sent to a centralized email address of SSI@tsa.dhs.gov.

Administrative Discussion

STSAC Homeland Security Information Network Critical Infrastructure (HSIN-CI) Portal

TSA HSIN-CI Representative Kilian Thorin provided a brief presentation of the work being done to develop the STSAC HISN website that is now launched and live. A webinar is scheduled on November 12th at 1:00 pm to further explain the site and will feature a discussion about possible improvements. Mr. Thorin asked all Committee members to log in to the site, and once they have permission to update their contact information. He showed everyone the reference document library for SSI documents. Mr. Thorin's team embedded collaboration tools into the site to provide version control through the Check-Out/Check-In feature and to refer to a Version History if necessary. His team established a tool for virtual voting that includes options for adding comments and/or justifications for decisions. He will take suggestions for improvement that will go to Mr. Budhram for consideration.

Closing Remarks

Mr. Farmer, Ms. Hanson, and DAA Newhouse provided brief closing remarks. Mr. Farmer noted that advocacy emerged as one of the main themes today. He will do so for the shared objectives of industry and government reflected in the agenda and discussion. He wants the Committee to make a difference and implement ideas to yield benefits for surface transportation security.

EAA Fitzmaurice enjoyed participating in the inaugural meeting in July and this meeting has not disappointed her either. She remarked on the strong participation. Ms. Fitzmaurice found the presentations informative, not only shedding light on the issues but also including inconsistencies and opportunities for learning because not everyone knew what TSA did. She will take the message back about how to work with the surface transportation community, especially driving consistency and raising that bar. Ms. Fitzmaurice recognized the passion for various priorities and recommendations. There is a need to rack and stack the discussions from today because if everything is a priority, then nothing is. She agreed with the need to focus on what the STSAC can implement. Ms. Fitzmaurice also mentioned the STSAC two-year term, which she equated to a marathon in that the STSAC will not accomplish everything overnight— rather the Committee will need to drive up the pace and accelerate how government works. Ms. Fitzmaurice thanked APTA for a fabulous facility and thought maybe the new TSA HQ would be like this for future meetings. If this level of commitment continues, it will make this group very successful.

Adjournment

DFO Budhram, Jr. reminded the Committee that he will be looking for a possible date for the next meeting. Mr. Budhram adjourned the second meeting of the Surface Transportation Security Advisory Committee at 3:42 p.m.