Surface Transportation Security Advisory Committee (STSAC)

Meeting Minutes

February 16, 2023

Meeting Summary

The Transportation Security Administration (TSA) hosted the 15th meeting of the Surface Transportation Security Advisory Committee (STSAC) in a hybrid format consisting of both in-person participation at TSA Headquarters and connection via WebEx teleconference. The meeting was closed to the public. The agenda was provided to participants in advance of the meeting.

The meeting focused on subcommittee updates on implementation of approved recommendations. Also included were updates from the TSA Law Enforcement and Federal Air Marshal Service (LE/FAMS), Surface Policy Division, and Surface Security Operations.

TSA Administrator David Pekoske; Policy, Plans, and Engagement (PPE) Assistant Administrator (AA) Eddie Mayenschein; PPE Surface Policy Division Executive Director and STSAC Co-Executive Sponsor Scott Gorton; and the STSAC Chair Thomas Farmer and Vice Chair Polly Hanson addressed the Committee.

The government and industry co-chairs of the Security Risk and Intelligence Subcommittee, Cybersecurity Information Sharing Subcommittee, Insider Threat Subcommittee, and Emergency Management and Resiliency Subcommittee presented their respective subcommittee accomplishments, near and longer-term objectives and projected outcomes, and the foundations for future Committee topics of interest.

Call to Order

Before the formal start of the meeting, the STSAC Designated Federal Officer (DFO) Judith Harroun-Lord provided a brief explanation of the in-person and WebEx teleconference procedures. She called the meeting to order at 1:06 p.m. EST, proceeded with a roll call of the Committee members, and announced a quorum of members present. Additional participants were asked to email their names to STSAC@tsa.dhs.gov for an accurate record of attendance.

PPE AA and STSAC Co-Executive Sponsor Introductory Remarks

PPE Assistant Administrator Eddie Mayenschein and STSAC Co-Executive Sponsor Scott Gorton (PPE) Surface Policy Division Executive Director (XD) welcomed everyone and provided introductory remarks.

Mr. Mayenschein welcomed Administrator Pekoske, the Committee members, Chair Farmer, Vice Chair Hanson, and the Aviation Security Advisory Committee (ASAC) Leadership Chair Steve Alterman and Vice Chair Chris Bidwell to the 15th meeting of the STSAC. He expressed appreciation to all who joined in-person and online, and noted this was the first STSAC meeting of the new year, 2023. He noted that DAA and STSAC Co-Executive Sponsor Kristen Simonds was participating in Capstone and that she regretted she was unable to attend.

He acknowledged that the Committee reelected Mr. Farmer and Ms. Hanson as Chair and Vice Chair and offered his congratulations to them. He expressed he was looking forward to hearing from the subcommittees on their dedicated perseverance in achieving their implementation plans. He expressed his ongoing support as government and industry continue to work in concert to implement ideas that will yield improvements for surface transportation security.

Mr. Gorton extended a warm welcome to everyone. At that point, Administrator Pekoske entered the room and Mr. Gorton gave him the floor.

TSA Administrator Opening Remarks

Administrator Pekoske greeted everyone and conveyed appreciation for the opportunity to provide remarks at the STSAC meeting. He acknowledged the dedication of the members and values the hard work of the Committee and the subcommittees.

He began by congratulating Tom Farmer and Polly Hanson on their reelection as Chair and Vice Chair and reflected on their inaugural service, the Committee's confidence in them, and their willingness to continue serve in these roles.

As many of the members know, TSA has done a lot of work with cybersecurity in the surface transportation security sector creating a good baseline of cybersecurity protection and cybersecurity resilience within the critical infrastructure sectors. On the surface transportation side, TSA always follows up security directives with a rulemaking process. TSA has begun that process and issued an advanced notice of proposed rulemaking (ANPRM), which many of the Committee members contributed to with TSA's special consultation held in December 2022. TSA has received comments back and is now adjudicating those comments. TSA will then issue a notice of proposed rulemaking (NPRM), which is anticipated to occur in late summer. It is quite a time-consuming process. TSA really values the comments that people provide, and when comments from industry stakeholders and the comments from the public are combined, TSA has a more robust document. The Administrator acknowledged he really appreciates all the work the Committee has done.

The Administrator noted that there is more concern now than when TSA first started this process because threat vectors are still very much there and, in general, it's fair to say that the world has become an increasingly challenging place within which to operate both on the physical side and the cyber side. The Administrator assured the Committee that TSA's emphasis remains on both threat vectors and in keeping industry informed. The Surface Information Sharing Cell (SISC) has been stood up and it has been very successful to date. TSA is still getting it up into a cadence that will be appropriate for information sharing that TSA endeavors to have across a very great sector of government.

The National Cybersecurity Strategy is anticipated to be published in the next few days. It is now within the Executive Secretary's process for the President to review and sign after going through the many levels of clearance. The Committee members will see a lot of what TSA and industry have collaboratively done reflected in the approach.

The Administrator will return at the end of the meeting and has requested that opportunity be used for dialogue regarding anything mentioned during the meeting that the Committee would like to discuss with the Administrator, both for mutual information sharing and for his reaction and opinion.

The Administrator opened it up for any questions before the onset of the meeting. Hearing none, he requested the Committee promise they would have something to run past him when he comes back. He values the Committee's input and highlighted that it helps him understand more fully the surface industry concerns and needs, so that he can improve the course of action across the surface transportation sector.

He looked forward to rejoining everyone later that afternoon and turned the meeting back over to DFO Harroun-Lord, who congratulated Chair Tom Farmer and Vice Chair Polly Hanson on their reelection and turned the meeting over to them for their opening remarks.

STSAC Chair and Vice Chair Opening Remarks

Chair Tom Farmer appreciated the great turnout for today and thanked everyone for their votes of confidence in reelecting him and Vice Chair Hanson to a second term.

He noted there is probably no greater recognition than to be doing something productive together and to be elected to serve in this capacity by highly regarded and respected peers.

He recounted a baseball story about the galvanizing moment when the Mets rallied from being in last place to win the pennant and the World Series. He noted that, in the professions we work in, we are faced with galvanizing moments all the time. It can be a cyber-attack, a shooting in a subway station, a disruption to pipeline operations, activists blockading trains. He noted that we assemble here to take those galvanizing moments and translate them into outcomes—to know that how we respond, how we prepare for, and how we prevent those galvanizing moments is better because of what we've done here. That being said, our goal today is to take some of the more difficult issues and apply the advantages of your collective expertise and experience to galvanize how we address and overcome challenges and impediments. He encouraged everyone to ask questions and offer comments from their unique perspectives.

Vice Chair Hanson expressed her appreciation for everyone's confidence in reelecting them to the roles of Chair and Vice Chair, and also acknowledged the robust attendance, both in the room and virtually. She highlighted that three years ago when the world shut down in March of 2020, while many had the luxury of remaining at home, those people who were declared essential workers had to come in and provide the goods and services that are so important to our way of life. As the pandemic progressed, the non-medical people, those people in our industries, were recognized as heroes. She wanted to talk about heroes because two weeks ago, a transit worker, Mr. Robert Cunningham, was killed trying to protect a passenger on a bus from an assailant; the attack started on a bus and ended on a subway platform. She highlighted that to say she is

honored to be with you, honored to be a part of this industry, and honored to be part of a group that is focused on the work we are doing because there are people like Mr. Cunningham who we work with and are out there every day supporting our customers and the communities that they serve. The work that we do in this Committee is so important because it has the ability to make them safer and more secure. She thanked everyone for their efforts and for being here today.

DFO Harroun-Lord thanked Chair Farmer and Vice Chair Hanson, and introduced Mr. James Cook, Mr. Darnell Young, AND Ms. Wanda Davis to present the Security Risk and Intelligence Subcommittee brief.

Security Risk and Intelligence Subcommittee

The Security Risk and Intelligence (SR&I) Subcommittee Industry Co-Chair and Assistant Chief of Police of the Amtrak Police Department James Cook opened the presentation with an update to the Committee on a specific area of concern and challenge—Surface Information Sharing Cell (SISC) membership.

The approval and signature of the SISC Charter by the Transportation Systems Co-Sector Risk Management Agencies (Department of Transportation and Transportation Security Administration), the Surface Sector Coordinating Councils, and the Pipeline Security Working Group in October 2022 was a key governance step in the expansion of the SISC and moving it to full operational capability.

The Subcommittee realized that additional guidance and processes were needed to expand the SISC membership with industry, federal government, and state, local, tribal, and territorial partners. The Subcommittee brief highlighted the steps taken to approve and implement the Surface Information Sharing Cell Charter. These actions have included a focus on the membership process, why SISC membership is significant, and the steps that have been put in place to mitigate member concerns and challenges.

The SR&I Subcommittee DFO and Chief of the SISC Darnell Young briefed the Committee on SISC membership, and the SR&I Subcommittee Government Co-Chair Wanda Davis provided an update on options for a Surface National Intelligence Manager.

Mr. Young welcomed new faces and thanked everyone for their support, looking forward to working with the new members.

Once the SISC Charter was signed, TSA had a lot of industry stakeholders, not only locally but all across the United States, asking how to join the SISC. Subsequently, the most significant challenge is expanding surface industry and government stakeholder's membership in the SISC as documented in the SISC Charter. Per the SISC Charter, industry and government council approval is needed for membership and participation in the SISC.

The feedback from surface transportation stakeholders indicated follow-up information was needed on a process for stakeholders to apply and/or recommend someone for membership. Also, information and/or guidance for the Government Coordinating Councils and Sector Coordinating Councils (GCC/SCCs) to approve membership in the SISC was needed.

Increasing the SISC membership is significant and impactful because it will give more surface transportation stakeholders with a need-to-know greater access to current and future surface and cyber products that the SISC is sharing on a daily basis. It will also allow for greater two-way discussions and information sharing on threats to surface transportation including cyber threats.

Developing an approved SISC membership process to properly vet and attain the approval of Government Coordinating Councils and Sector Coordinating Councils (GCC/SCCs) for the wide range of surface transportation stakeholders requesting membership is a challenge. This challenge is being mitigated by the production of a one-page SISC Fact Sheet and information-guidance documents on becoming a SISC member and is currently going through the internal TSA approval process. We anticipate distribution of the SISC Fact Sheet in the next few weeks.

These two documents will be distributed to surface stakeholders, to include State, local, tribal, and territorial (SLTT) stakeholders, via the industry and government modal councils; TSA Industry Engagement Modal Managers; TSA Surface Operations; and TSA I&A Field Intelligence Officers. The documents are shared on HSIN and the SISC WebEx forums held twice a week. These actions will help facilitate increased SISC membership and access/participation in the following information sharing forums:

1. SISC quarterly Classified Surface Industry Days.
2. SISC Intelligence-Information WebEx updates (currently each Tuesday and Thursday with expansion to five days per week scheduled to begin the first part of April).
3. Greater access to surface and cyber relevant products on the new SISC Community of Interest (COI) page on the DHS Homeland Security Information Network (HSIN) anticipated in the next two weeks.
4. Increased access to classified documents at TSA HQ or in the field for cleared stakeholders.

Increased surface industry membership in the SISC also demonstrates the commitment and structure that warrant the step of presenting the STSAC request for a Surface National Intelligence Manager (NIM) to the Office of the Director of National Intelligence (ODNI) dependent on the Department of Homeland Security (DHS) Chief Intelligence Officer (CINT) concurrence.

Mr. Young introduced the SR&I Government Co-Chair Wanda Davis to present an update on options for the Surface National Intelligence Manager.

On January 9, 2023, Ms. Davis and DFO Darnell Young met with Deputy National Intelligence Manager (NIM) Western Hemisphere (WH) to provide an overview of TSA I&A Threat Intelligence Sharing Branch and SISC mission and to explore the potential for NIM advocacy for Surface information sharing.

NIM-WH was gracious and understood our efforts. They said the NIM-WH has a small critical infrastructure portfolio but can serve as a starting point and help identify other NIMs with larger critical infrastructure portfolios, which may be able to serve as potential advocates. The January 9 initial outreach with NIM-WH office helped meet the following two main objectives:

1. Familiarize NIM-WH office with TSA's I&A/TISB intel sharing mission and efforts; and

2. Explore opportunities for future collaboration with NIM-WH and other potential NIM offices that could help advocate surface intelligence requirements at the Intelligence Community (IC) level.

For the way ahead, the SISC will re-engage with the NIM-WH for follow-on discussions and will invite the NIM-WH and Deputy NIM-WH to attend our upcoming SISC Industry Day on April 4, affording the opportunity for them to observe directly the kind, and caliber, of work that we do with the surface transportation industry and to provide further insight into SISC's intelligence-threat information sharing efforts, challenges, and opportunities. Ms. Davis opened the subjects presented to questions.

Chair Farmer asked how many requests had been received for membership. Mr. Young replied to about 40 requests for membership were received and, as yet none has been submitted to the SCC/GCCs. He explained that the SCC/GCCs have requested TSA provide them with the official membership process, documents, and guidance approved by TSA Chief Counsel's office. Once the official membership process with the Fact Sheet and membership guidance is approved by TSA Chief Counsel's office, TSA will provide these criteria to the Government Coordinating Councils and Sector Coordinating Councils (GCC/SCCs) to use for selection. While the Charter lays out the process, the Fact Sheet and membership guidance give specific steps and basic requirements for SISC membership. The majority of stakeholders will be able to apply to the SCC/GCCs, which will make a decision based on reviewing the applicant's position and responsibility. TSA also will vet applicants to ensure they meet the basic need-to-know criteria that is required in the nondisclosure agreement before the SCC/GCC actually approves them.

Ms. Davis explained how TSA processes membership requests for the Air Domain Intelligence and Analysis Cell (ADIAC) on the aviation side.

Mr. Farmer wondered if it would facilitate the process if the SCCs made nominations—as their members and participants often already have the clearances and requisite need to know.

Mr. Young replied that the SCCs want to have the TSA-approved process before picking one or two modes and hope the process will be in effect by the next meeting. All surface modes will receive the Fact Sheet and guidance about how to apply. Surface transportation industry stakeholders can participate either with a Secret clearance or higher or if they have a need to know since a lot of people do not have the opportunity to get a clearance. When the process and documents are prepared and approved, modal SCCs, TSA PPE Industry Engagement Managers (IEMs), TSA Surface Operations, and Field Intelligence Officers (FIOs) will distribute to industry. TSA will also distribute via SISC WebEx briefs and HSIN. If there are additional groups that would benefit from membership, the SISC can certainly add them.

Mr. Young explained when I&A launched the SISC, they set up a pilot program with the STSAC industry representatives to initially build out the SISC because members were already vetted by TSA. Now there is a need to expand beyond the pilot program and the SISC team has reached out to DHS HSIN to expand the SISC to the broader community. Mr. Farmer commended the great work laying this out so far.

Ms. Davis added that the vision for expansion goes beyond welcoming in the broader community of industry stakeholders to include reaching out to government partners as well. For instance,

the NIM-WH could be a member. She encouraged industry to continue providing input and feedback, as it has created great value.

Mr. Farmer noted that, as SISC membership expands, participation in SISC Industry Days will far exceed what TSA HQ can host in a single secure room. He observed that a larger venue would be needed as the SISC expands, as well as technological accommodations for those who cannot travel to TSA HQ for briefings to still be a part of the discussions, emphasizing professional demands that may preclude or limit opportunities to travel for a single day meeting.

DFO Harroun-Lord thanked everyone and introduced Mr. Tim Weston and Ms. Norma Krayem to present the Cybersecurity Information Sharing Subcommittee brief.

Cybersecurity Information Sharing Subcommittee

The Cybersecurity Information Sharing (CIS) Subcommittee Government Co-Chair Tim Weston greeted everyone, expressing appreciation for the space at TSA HQ that allows for robust meetings and dialogue.

He opened the discussion focusing on CIS Recommendation #2: "*Manage the operations of the SISC under the express authorization of the Cybersecurity Information Sharing Act of 2015*." This federal legislation expressly authorizes sharing of information on cyber threats, incidents, and security concerns—between industry and government, within industries, and across critical infrastructure sectors; and affords protections against anti-trust and civil liability, Federal FOIA, and state/local sunshine acts for information sharing authorized by its terms.

The Subcommittee had been asking TSA officials to confirm whether or not CISA/2015 Act protections apply to sharing under the SISC as well as whether or not the same protections apply to those regulated by the existing TSA Security Directives.

The CIS Industry Co-Chair Norma Krayem provided background and context for why the Subcommittee was asking these important questions. The CISA/2015 Act provided limited liability protections as well as protections against Federal FOIA, state and local sunshine acts and more, meaning those that submit information directly to CISA are given these protections. However, information provided to TSA through the SISC would not necessarily be covered by that and the Subcommittee asked TSA's Chief Counsel's Office to provide legal clarification. The CIS Industry Co-Chair Norma Krayem further explained the rationale. The legal protections afforded by CISA/2015 Act are critical to owners and operators. Assurance is needed that those protections cover information shared with the SISC. If that is not clear, then entities may not share information with the SISC fearing legal ramifications. As the SISC membership expands, providing an opportunity to reach more people with an expanded venue from which to share more information becomes more and more critical.

Mr. Weston noted TSA has said it believes that any sharing of information to the SISC is also covered by CISA/2015 Act protections. This position can and should be conveyed clearly to all stakeholders by TSA. Once that step is implemented, this recommendation can be closed out.

Ms. Krayem then discussed a related question on which the Subcommittee has focused – whether the CISA/2015 Act authorizations and protections also apply to information shared under the TSA Security Directives to CISA. The CISA/2015 Act precludes use of cybersecurity information shared with CISA for regulatory purposes, while reporting mandated under the SDs meets a regulatory purpose. She emphasized that industry needs legal clarification on what protections exist under CISA/2015 Act when mandated to report cyber incidents under the SDs to CISA. Industry would like to see action taken on this priority with support from TSA—to understand how CISA and TSA are working together and to clarify that there is no regulatory reach back and to clarify the legal/FOIA protections.

Mr. Weston noted that even during the recent CIS Subcommittee that hosted a speaker from the Joint Cyber Defense Collaborative (JCDC), there was some level of uncertainty within the JCDC as to how this works from the CISA side. Support is needed from TSA's and CISA's Chief Counsel Offices to resolve these questions for industry. If these offices need clearer information about the questions industry has, the CIS Subcommittee can help share specific questions, however; the basic questions are clear.

Separate from these questions, Ms. Krayem discussed the work by the CIS Subcommittee to bring in additional DHS speakers to discuss CISA programs to help industry better understand how the two agencies are working together and to work to avoid duplicative structures without clarifying what the roles are under CISA.

Mr. Young reinforced the clarification and distinction that the SISC is really a collaboration between multiple government offices and industry. The SISC is not resourced to be an analytical cell, rather it is designed to distribute and share information. The SISC's success thus far is the result of this collaboration.

In response to Vice Chair Hanson's inquiry as to who is helping them, Mr. Weston replied that since these issues have been brought to the forefront over the past few months, the Subcommittee has reached out to the TSA Chief Counsel's Office and those in the SISC to set up discussions. They envision, and encourage Subcommittee members to help further refine the thinking with their participation and input on these specific concerns.

While the first step is working with the Chief Counsel's Office, Ms. Krayem reached out to the entire STSAC to send other questions related to this issue so the CIS Subcommittee can compile a full list for review with the lawyers. Ms. Krayem noted the CIS Subcommittee may have an update by the next meeting.

Mr. Weston added that enabling information sharing through the SISC has a very specific purpose—to share cybersecurity information with the intent that it flows into the SISC, gets shared, and sent back out to cybersecurity practitioners.

Mr. Weston clarified that the SISC is not only reviewing incident-related information required to be reported through the security directives, but also covering physical security and cybersecurity information outside of the SDs to ensure it is funneled correctly.

Mr. Weston mentioned that TSA issues security directives and couples FAQs with them. Including the FAQs as part of the document may be a way to work going forward.

As a follow-up comment, many industry partners will want these questions answered before they agree to take part in the SISC. It was recommended that updates and FAQs on these issues be added to the SISC membership package to help explain these issues in more detail.

Mr. Grandgeorge pointed out that TSA partners might consider having a conversation about how they process and compile information. For instance, from the industry perspective, the recently published Pipeline Modal Assessment, designated as Sensitive Security Information (SSI), was incomplete because it did not include information about an individual who had pleaded guilty to terrorism against the pipeline community within a week of the assessment being issued. He hoped the SISC might help in some way to support the development of the Modal Threat Assessments – by enabling industry input as they are developed – to enhance engagement by TSA partners with industry.

Chair Farmer pointed out that clarity critical to ensure that mandates on reporting that apply to multiple surface modes do not undermine effective practices for information sharing – within modes, across modes, and across sectors. Some organizations covered by the TSA Security Directives have stopped sharing information on cybersecurity incidents they are mandated to report to CISA. Their reasoning – with the directive, the decision on further sharing is no longer their; rather, it is for the government to determine. If an organization is going to share with the SISC, we will have to restore confidence that the mandates on reporting in the directives are not an impediment. Again, the sense is that, because it's a requirement under an SD to report to CISA, an organization is then precluded, or at least reluctant, to do anything else with it.

Ms. Krayem added that organizations can still share information with the Information Sharing and Analysis Centers (ISACs) or other organizations because the CISA/2015 Act lays out clearly conveyed protections. This venue would ensure the information gets out.

Chair Farmer further defined this issue. Industry needs clarification. The CISA/2015 Act applies specifically to reporting and sharing information on cyber incidents, threats, and significant security concerns. The SISC and ADIAC can anonymize the information and then share it—that is the benefit: industry entities send in the information, the SISC or ADIAC strip it of identifying details, and then they send it back out with some analysis and security recommendations. If we can work to come to an agreeable means of clarification, the result will be a progressively expanding level of early sharing of cybersecurity information to enable actions to narrow risk profile. That is something that the SISC body can help with, by working with leadership to convey this clarity.

STSAC Co-Executive Sponsor and PPE Executive Director Scott Gorton noted that he had been thinking about how TSA might address these issues. He clarified that some entities covered by the SDs are required to report certain types of incidents. Reporting is very different from sharing, which is a voluntary act between parties to alert them. Incident reporting is a mandatory requirement to report certain events to the federal government so that they can look for trends. Is there an interpretation right now among the covered parties that reporting precludes from sharing with industry?

Members discussed further that when something happens, there is a very quick determination about whether or not it is a reportable event. If it is decided that an incident does not meet the intent and the entity need not report it, they also do not want the company to share that on a forum like the SISC because of the potential for misinterpretation. Pipeline/rail/electric already formed other groups to share information. While comfortable, this is not as broad and beneficial. Industry has put together their own silos, and the SISC is trying to break out of and expand beyond that. We need to get through this barrier.

Mr. Gorton noted that the government is not combing the bushes for voluntarily shared information and then using that for enforcement. There were similar concerns expressed 10 years ago regarding the reporting requirement for physical security and fear that TSA would take a compliance approach to see what they could enforce. In the last 10–15 years, TSA has not pursued any cases unless there was a willful and knowing intention to hide information. There has been more consideration of misinterpretations as to whether or not something met the reporting threshold. Mr. Gorton noted that he will take that for action and clarify this in an FAQ about how the federal government uses the information they are asking/requiring entities to report and that they are not trying to stymie the good practice of sharing information.

Ms. Krayem thanked Mr. Gorton and noted that was exactly what industry needs to hear.

Deputy Chief Counsel for Regulations and Security Standards Susan Prosnitz underscored that point after listening to the discussion, noting it will be helpful to provide that clarifying information in an FAQ. She will circle back as a legal team and work with Mr. Gorton's team to get clarification out to the industry.

DFO Harroun-Lord thanked everyone, and introduced Mr. Joseph Perez, Mr. Koi Hallonquist, and Mr. Linwood Guise to present the Emergency Management and Resiliency Subcommittee brief.

Insider Threat Subcommittee

The recently appointed Insider Threat (InT) Subcommittee Industry Co-Chair Joseph Perez opened the discussion with a brief introduction highlighting his 10 years in the security community and his 28 years with the Illinois State Police Department. Chief Perez is an inaugural member of the STSAC and is honored to have been selected as the Industry Co-Chair of this Subcommittee. Understanding what we are doing here is bringing the best partnerships together to solve problems, Chief Perez sees the next step to be the opportunity to bring together public/private security industry professionals who have established procedures that can bring these practices to bear. One of the important things to push forward is the Insider Risk Mitigation Hub (IRMH). Chief Perez turned it over to Mr. Koi Hallonquist to discuss the IRMH.

The Insider Threat Subcommittee Government Co-Chair Koi Hallonquist greeted everyone and noted he is also a new member of the Subcommittee and a new member of the Insider Threat Program leadership team along with Lynwood Guise. Mr. Hallonquist is taking over for Scott Carpender and expressed his appreciation for Mr. Guise, as he has relied heavily on him during this transition. Mr. Hallonquist noted he is excited to move the Insider Threat Program forward by supporting the implementation of the Insider Threat recommendations.

Mr. Hallonquist brought forward the InT Recommendation #3, "*Expand the newly established Insider Risk Mitigation Hub (IRMH) by integrating surface transportation industry representatives and leveraging the combined expertise of public and private security professionals*" for discussion.

Based on the TSA Administrator's 2020 Insider Threat Road Map /Priority 2 to Advance Operational Capability and 2.2 Establish an enterprise-level, centrally managed capability to integrate, analyze, and respond to potential insider threat information, the vision was for TSA to establish an Insider Threat Mitigation Hub to elevate insider threat to the enterprise level and enable multiple offices, agencies, and industry entities to share perspectives, expertise, and data to enhance threat detection, assessment, and response across the Transportation Systems Sector.

The initial scope for the IRM Hub brought subject-matter experts from multiple internal TSA bodies together in collaboration to detect and deter applying enterprise risk-mitigation efforts. The Hub now provides the overall insider threat management and development for TSA threat analysis of the insider threat risk indicators and long-term trends. Inquiries and investigative support all occur in the Hub. Currently the members of the Hub include core offices within TSA—LE/FAMS, I&A, Investigations, SO and IT Information Assurance Division. The IRMH has a robust TSA participation and is now looking to bring industry in to meet the goal of this Subcommittee—moving forward to incorporate industry into the Hub.

Mr. Hallonquist highlighted recent accomplishments within the Insider Threat Program. TSA has developed the Case Management System that deploys analytic capabilities in the form of the Case Optimization and Risk Evaluation (CORE) tool, a capability that runs on top of software analytics and incorporates specific potential risk indicators (PRIs) that are very specific to transportation.

TSA recently awarded and executed a contract with a locally owned small business to provide programmatic support services to the Insider Threat Program. These services enable foundational document updates and procedural advancement of TSA's Case Management System and CORE tool, which should facilitate mechanisms for incorporating industry representatives.

All contractors have been on-boarded and are working out of the IRMH. The Insider Threat Program will incorporate industry from the beginning as we develop the policies and the SOPs for the Risk Mitigation Hub. The IRMH envisions bringing on full-time detailees with different classification levels to the project, focusing on what risk and mitigation SMEs can bring to the table to strengthen our analytic capabilities and industry's as well. Enhancing information sharing is a priority also—to be achieved by working collaboratively with our Insider Threat Section personnel and other stakeholders to support Insider Threat inquiries, investigations, and assessments at airport or surface worksites.

First steps are identifying the current state of industry stakeholders' programs and the needs on both sides, industry and government. The IRMH would like to identify POCs for industry insider threat programs and provide procedural updates and documentation generation, which will help the IRMH design its policies and procedures. Mr. Hallonquist handed it over to Mr. Lynwood Guise to continue explaining the project.

Mr. Guise summarized—the Hub was stood up in 2019 with participation across all TSA offices, some in administrative roles and others in operational roles—assisting in operations, investigations, and conducting inquiries. The focus now is to expand that membership to include industry stakeholders who will bring in a unique perspective that TSA can leverage in getting information back and forth for information sharing, as well as how we can best mitigate risk in those different industries. First steps are to identify the current state of industry insider threat programs and then to identify points of contact so TSA can reach out to established industry partners for their input in their next phase when they start developing policies.

Vice Chair Hanson asked how they intend to do outreach, get the POCs, and identify the state of their insider threat programs.

Mr. Guise responded they are definitely working through the Insider Threat Subcommittee partners and, as the Administrator has recommended, are leveraging boots-on-the-ground equities as well. That information will be passed back and TSA will be the repository for that.

Mr. Adam Long acknowledged Mr. Hallonquist and Mr. Guise for standing up this initiative. He noted that, in the Energy Sector, insider threat is the top threat faced every day. To that point, owner/operators have partnered with electric industries that also have this as their number one threat such as physical attacks on transformer sites and attacks on the eclectic grid. The electric industry and the Federal Energy Regulatory Commission (FERC) have been working in this space for several years and have compiled a lot of resources. He noted it may be a good starting point to look at what resources have been put together as well as who those established points of contact for industry experts are who have been down this path in different modes of transportation. Part of the situation is to catch up with industry and then help lead them going forward from that. There are some resources there; he offered to talk later about how to access.

Mr. Guise responded that is exactly the input TSA is looking for. If it's not broken, don't fix it. TSA needs to take that snapshot of the as-is first in order to partner with industry on designing the plan.

Mr. Long agreed to the importance of this Hub bringing everyone together to identify not only what's being done, what the different modes' needs are, what's attainable, before putting together a package of options.

Mr. Daniel Krantz noted he completely agrees with what Mr. Long said and can only add to it. One of the things that's really important here is to not circumvent some of those independent efforts that are already started, rather to embrace and incorporate them into what is being developed.

PPE AA Eddie Mayenschein joined the conversation on the IRMH and recommended that the TSA Insider Threat leadership team also engage with PPE's Industry Engagement Managers to support stakeholder outreach on the IRMH effort. He noted recent examples of successful industry collaboration, such as TSA's partnership with the pipeline industry to identify and develop performance-based cybersecurity policies. In a similar fashion, TSA can engage with stakeholders to obtain their insight on effective insider threat programs and practices, while also accounting for differences across industry.

Chief Perez concurred that many good programs already exist. Insider threat is usually about a person or a small group of people and there is a tremendous amount of wonderful professionals who are doing the right thing every day. To Mr. Mayenschein' s point, no one wants to go back and discount or disavow the great work that's been done, and that's another important reason for not being too prescriptive.

Mr. Guise added that there's never been a training session that he's attended where industry wasn't the largest represented group. Their programs are very mature; TSA recognizes that and wants to know how can we help.

Mr. Guise elaborated the IRMH team would be introducing and explaining the program. Most of TSA's partners don't know TSA has an Insider Threat Program and that we have resources we can provide. The Insider Threat Program is working with PPE right now to develop materials that can be left with industry highlighting what the TSA Insider Threat Program does, this is how you contact us, and this is how we can help.

Chair Farmer thanked Mr. Guise.

DFO Harroun-Lord thanked everyone, and introduced Mr. Robert Gatchell and Mr. Chris McKay to present the Emergency Management and Resiliency Subcommittee brief.

Emergency Management and Resiliency Subcommittee

Emergency Management and Resiliency Subcommittee Industry Co-Chair Robert Gatchell welcomed everyone and extended his thanks and congratulations to Chair Farmer and Vice Chair Hanson on their continued tenure.

He updated everyone that the Subcommittee had convened several meetings in December and January to discuss potential new topics and has focused in on a significant area of interest: potential impacts to the surface transportation community that could result in the event of a disruption to the power grid as the surface community continues to transition to cleaner technology.

This is an important area because of a number of variables:

- The surface transportation enterprise has begun or will begin to transition to cleaner technologies over the next 5–10 years.
- There is significant and increasing reliance on the energy grid/power as this infrastructure is built out.
- There are cost challenges in building out this infrastructure.
- There are significant cascading impacts to the sector in the event of a power disruption.
- There are evacuation challenges.

Subcommittee discussions covered a plethora of challenges, cascading effects, developing mitigation strategies, and the escalating concern over domestic violent extremists (DVEs) and various plots/attacks that have surfaced in the past several years. Mr. Gatchell turned it over to the EM&R Government Co-Chair Chris McKay to continue the conversation.

Mr. McKay expanded on the area of interest and discussed next steps going forward. The Subcommittee is planning an unclassified Webinar with the surface transportation community on March 15 to provide awareness and an overview on the current state of the power grid and the potential impacts to the surface transportation community that could result in the event of a disruption. Agenda Topics are the Energy Sector and Power Grid Overview, Unclassified Intelligence Briefing (power grid) from the Department of Energy, Industry Perspectives, and Open Discussion.

Participants will include representatives of surface transportation entities, relevant associations, Federal Government partners, and other interested parties, notably the transit community and over-the-road bus as stakeholders who continue to evaluate the challenges associated with integration of cleaner technology, as well as pipeline professionals to understand the cascading impacts to their organizations in the event of a disruption.

Tentative presenters are the Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response; Peter Pan Bus; American Public Transportation Association; and Duke Energy.

The Subcommittee will develop and distribute a 2023 Power Grid Workshop After Action Brief to share across the surface transportation community after the webinar and the Subcommittee will brief out the results at the quarterly STSAC meeting in May.

Mr. McKay asked if other subcommittee members had anything to add or if there were questions.

Mr. Young expressed an interest to take part in this initiative because there have been two-way discussions on this topic during the SISC WebEx Intelligence Briefs. He referenced a resource paper regarding the extensive power outages in the Houston area after a major ice storm.

Ms. Krayem inquired if they were also looking at cybersecurity risks and their cascading impacts. That would mean that some parts of surface transportation wouldn't be able to operate.

Mr. McKay acknowledged that point as an excellent idea and noted it could certainly be on the table. Ms. Krayem offered her help as necessary.

Chair Farmer accredited the good work being done and noted the audience might extend beyond surface transportation to include the Energy Sector and any entities with substantial reliance upon electricity for resilient operations. There will be a lot of material to support and develop a Quick Look report.

Vice Chair Hanson joined the conversation and highlighted that one of the speakers is going to discuss all-electric vehicles and, in particular, planning for an outage in Florida because the organization has responsibilities to help with hurricane evacuations. She emphasized how important it is to have these conversations ahead of time to know what the resources are available, not just for ice storms, but also for brown-outs in California because of the heat. Expect to find interesting things during the webinar.

DFO Harroun-Lord thanked everyone and informed participants that an Unclassified Threat Brief would be presented after a 20-minute break.

BREAK

Threat Briefing

Analysts with TSA's Intelligence and Analysis Office provided current threat briefings to the STSAC membership. The I&A analysts presented an overview of terrorist threats to the surface modes of transportation in the United States and then discussed current cyber activities, cyber actors' intent and capability to conduct attacks, and historic cyberattack trends that have affected U.S. transportation.

(Note: At this point, Administrator Pekoske rejoined the meeting in time for the next presentation.)

DFO Harroun-Lord thanked everyone and introduced TSA LE/FAMS to present the LE/FAMS update.

LE/FAMS VIPR/JCC Program Update

Supervisory Federal Air Marshal in Charge (SAC) Bob Bond and Deputy Supervisory Federal Air Marshal in Charge (DSAC) Nick Rock with TSA's Law Enforcement/Federal Air Marshal Service (LE/FAMS) provided a Visible Intermodal Prevention and Response (VIPR) program update to the STSAC membership. SAC Bond and DSAC Rock presented an overview of the VIPR program's law enforcement mission and team management, their efficient risk-based CONOPS that drives metrics and VIPR team deployments, and their success stories.

DFO Harroun-Lord thanked everyone and introduced Chair Farmer to present the Committee Administrative Discussion.

Committee Administrative Discussion

Committee Vote for November 17, 2022, Meeting Minutes

Chair Farmer led the Committee vote to accept the November 17, 2022, meeting minutes as distributed to members in advance of the meeting. Mr. Farmer requested a motion to accept the minutes. Chief Perez moved to accept the minutes and the motion was seconded by Mr. Long. The motion carried by voice vote and the minutes were accepted.

TSA SO Surface Operations Update

Security Operations (SO) Surface Operations (SO) Assistant Administrator (AA) Sonya Proctor graciously conceded her time to allow for continuing the robust and interactive discussions.

TSA OS Surface Policy Division Update

Executive Director Gorton took questions only in the interest of saving time after the robust discussions earlier. He mentioned the advance notice of proposed rulemaking (ANPRM) on surface cyber risk management and the request for pipeline, rail, and rail transit stakeholders to share their thoughts on the range of topics raised and questions posed. Trade associations weighed in with the common themes of "don't reinvent the wheel, don't be prescriptive, acknowledge consistent standards," and, most frequently, "follow the National Institute of Standards and Technology (NIST) framework," since many companies have built their own performance and benchmarks around its guidance. Mr. Gorton stated that TSA is continuing to carefully look at all the input, but agreed with these points, and anyone who read the SDs would see portions of the NIST Cybersecurity Framework in their requirements. Overall, he found the commentary helpful and had stood up a team to go through it all. Over 400 individual comments from 36 entities came in as a response to the *Federal Register* notice, so it would take the team time to go through all of those.

Ms. Hanson commented about the funding necessary to implement the rulemaking, identifying a potential economic burden for creating a robust program. The government should plan on earmarking support through direct grants or other means of assistance. She recognized TSA is trying to do this to the best of the agency's ability.

Ms. Krayem worked hard with CISA through her subcommittee, concentrating on harmonization. They assisted with a report that came out through the Cyber Incident Reporting Counsel (CIRC). Plus, CISA has a number of products they kept pushing out, and they've given the subcommittee a briefing about these, but she hoped to focus efforts on surface transportation in general.

Administrator Pekoske explained that the harmonization effort encompassed the entire federal government, with the national cyber strategy would set the stage for that; he expected its release within the next few days. Quite significant differences for reporting requirements existed across the government. CISA has the lead for implementing what Congress has required with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022. That statute, which remains to be implemented through regulation, has set 72 hours for reporting cybersecurity incidents. Harmonization efforts went beyond reporting and towards performance-based rules; he did not envision the government returning to something very prescriptive. With respect to the products released, they proceeded from discussions with sector risk management agencies and positioned CISA as a place where owners/operators could go for assistance without the concern of a regulatory penalty relating to their request ensuing, such as for reporting. CISA, TSA, Coast Guard, and DOT shared the transportation sector, so each agency could help with one area and rely on another's capabilities for any gaps. Some of the work might require changes to presidential directives, but the national cybersecurity strategy rollout would give them more direction. TSA continued to focus on improving cybersecurity in the Transportation Sector. Also, a liaison at CISA from TSA had established good communications, as well as positive relationships, between the modal managers and DOT, enough so that Administrator Pekoske considered placing another liaison officer over at DOT because of all the work we do across the modes—as a direct conduit for questions, since the agencies fall into two different cabinet departments.

Chair and Vice Chair Closing Remarks

Vice Chair Hanson closed by saying that while she doesn't know anyone who says they want to go to more meetings, she found the STSAC quarterly events good to attend. Today she heard about great work being done by the right people and thanked everyone for that.

Chair Famer noted that we hoped to generate a lot of comments and discussion when adjusting the subcommittee presentations for the first time to focus on key topics of concern that each subcommittee has and thought that this approach yielded very productive discussions. He came away with several areas for follow-up, including highlighting the process for joining the SISC, the outreach on seeking appointment of a Surface National Intelligence Manager, questions raised about reporting and alleviating some concerns and the need for documentation clarifying this, focusing on the surface industry's expanding reliance on the electric grid, not reinventing the wheel for insider threat, plus that subcommittee's good plan for outreach. Mr. Farmer looked forward to what would follow to help industry understand the insider threat hub (IRMH). He appreciated the brief on the electric power grid, the intelligence briefs, and LE/FAMS program update, and found the overview of cyber incident reporting in transportation as the best he had heard so far, as it helped to understand what surface transportation colleagues experienced and know what counted as reportable. He predicted that shifting from annual to quarterly approaches would prove very beneficial.

TSA Administrator Closing Remarks

Administrator Pekoske found it good to see so many people and highlighted the benefit of hybrid in-person and WebEx meetings. He observed that the robust and candid dialogue made him glad as it reflected what the advisory committees are designed to do. He noted each member plays an integral part in the STSAC and brings a wealth of experience and expertise to the table. What you say at these meetings and at the subcommittee meetings has significant bearing on our actions going forward.

Commenting on what Chair Farmer said, on the SISC, he completely supports the idea that expanded membership is very desirable and we want to make the SISC a robust information exchange, more so than it is today.

With respect to insider threat, he noted it's a threat vector all of us are very concerned about. TSA sees it every single day, both on the aviation side and the surface side, and it's a vexing problem. He noted we could learn from each other on how to approach this issue. Here is where the SISC would also help convey information about trends with insiders. As strengths increase in certain areas, everyone must stay mindful of unaddressed threats because perpetrators eill attempt to find and go through the path of least of resistance. For instance, everyone found it very hard to get advanced information about Domestic Violent Extremists.

On resourcing and managing expectations, he candidly did not see the federal government providing resourcing for measures that are required in the security directives. He did not want to establish the expectation that the regulations would be covered through grants or other funding. He noted TSA can provide support and stressed he wanted to be realistic, acknowledging that agencies are very constrained as is industry. He thought the key would rest instead on giving industry enough time to budget cybersecurity within their own organizations.

He aimed to have his staff provide feedback on cyber implementation plans as they came in to lessen the learning curves for others while keeping the sources anonymous to guard proprietary information. He urged attendees to look at their own plans and make adjustments. With a performance-based focus and sharing of best practices, companies would collaboratively share anonymized information to keep up with the technology without having to worry about the process.

Administrator Pekoske concluded by expressing a desire to attend more of the next meeting, particularly during the subcommittee reports, to hear what went on there.

Adjournment

DFO Harroun-Lord sought a motion to adjourn the meeting. Mr. Chris Engelbrecht motioned to adjourn the meeting. The motion was seconded. The motion to adjourn was carried by a voice-vote of the Committee.

The 15th meeting of the STSAC meeting was adjourned at 4:15 p.m. EST on February 16, 2023.

Certification of STSAC February 16, 2023, Meeting Minutes

I hereby certify that this is an accurate record of the activities of the Surface Transportation Security Advisory Committee on Februrary16, 2023.

Thomas L. Farmer
Surface Transportation Security Advisory Committee Chair