Surface Transportation Security Advisory Committee (STSAC)

Meeting Minutes

May 17, 2023

Meeting Summary

The Transportation Security Administration (TSA) hosted the 16th 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 TSA Intelligence and Analysis, DHS Counterterrorism Center (CTC), TSA Surface Policy Division, and TSA Surface Security Operations.

TSA Senior Official Performing the Duties (SOPD) of the Deputy Administrator Stacey Fitzmaurice; Policy, Plans, and Engagement (PPE) Deputy Assistant Administrator (DAA) and STSAC Co-Executive Sponsor Kristen Simonds; PPE Surface Policy Division Executive Director and STSAC Co-Executive Sponsor Scott Gorton; Security Operations (SO) Surface Operations (SO) Assistant Administrator (AA) Sonya Proctor, 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 12:07 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.

STSAC Co-Executive Sponsors Introductory Remarks

STSAC Co-Executive Sponsors Scott Gorton and Kristen Simonds welcomed everyone and provided introductory remarks. They acknowledged the team for making the arrangements/preparation.

Ms. Simonds informed the committee that she is leaving TSA for a position with the Federal Aviation Administration by the end of the month. She expressed that she is honored to have served as the PPE Deputy Assistant Administrator (DAA) and STSAC Co-Executive Sponsor.

She welcomed and introduced the incoming PPE DAA Robert Vente, who currently serves as the Regional Director in Europe for International Operations and will assume the role of Co-Executive Sponsor of the STSAC.

She then introduced Senior Official Performing the Duties (SOPD) of the Deputy Administrator Stacey Fitzmaurice.

TSA SOPD of the Deputy Administrator Opening Remarks

SOPD of the Deputy Administrator Stacey Fitzmaurice thanked everyone for joining us today and offered a special welcome to those able to be with us at TSA headquarters. She recognized that Administrator Pekoske was unable to join us today and she extended his greetings and appreciation as well.

Ms. Fitzmaurice highlighted the critical collaboration between TSA and industry stakeholders, noting the critical, integral effort that provides valuable knowledge and expertise that industry brings to the table as we tackle together the threat that we face in the surface transportation system. While we all recognize that it's a 24/7 life that is very difficult, it's about those partnerships and our collaboration that enable us to be successful in helping to prepare and protect the nations' transportation surface system.

Ms. Fitzmaurice acknowledged some of the important thangs that are going that continue to contribute to the ongoing success of the STSAC to include the following.

STSAC Annual Report

Ms. Fitzmaurice recognized the hard work being done on this year's Annual Report, acknowledging it is a significant lift to put such a comprehensive report together. She and the Administrator look forward to receiving it.

Cybersecurity Risk Management & Surface Vetting NPRMs

She highlighted two critical rulemaking efforts.

- First, in December 2022, and February 2023, the STSAC provided valuable industry input on the Advanced Notice of Proposed Rulemaking for the Cybersecurity Risk Management regulation.
  - TSA is presently considering industry and public feedback as TSA moves forward with the forthcoming Notice of Proposed Rulemaking (NPRM).
- Second, under the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA is required to issue a regulation requiring security vetting of certain public transportation, railroad, and over-the-road bus employees.
  - Under the proposed vetting rule, certain security-sensitive employees would undergo TSA security threat assessments that include checks against the terrorist watch list, of

immigration status, and of criminal history to determine whether the applicant may pose a security threat.

- o TSA expects that this NPRM will be published in the very near future for public notice and comment.

TSA looks forward to continuing to engage with the STSAC and the public as TSA develops these two critical regulations. Ms. Fitzmaurice thanked everyone for the work that has been done so far and thanked all in advance for their continued engagement in the development of these two very critical regulations.

Extension of the SD Pipeline-2021-01 Series: Enhancing Pipeline Security

TSA intends to extend the SD Pipeline-2021-01 series.

- This directive requires owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.

- TSA appreciates industry's continued collaboration as TSA develops a longer-term regime to strengthen cybersecurity and resilience in the transportation sector.

Acknowledgement of the Work of the Subcommittees

- Ms. Fitzmaurice took this opportunity to thank all of the Committee members who have been working so diligently along with our TSA staff to implement the recommendations of each of the subcommittees.

- Understanding each of these subcommittees have recommendations that are either in the process of being completed or are being prepared for formal closure, she and the Administrator look forward to receiving and reviewing these packages in the near-term.

TSA Budget Concerns

- Ms. Fitzmaurice noted she understood there have been concerns expressed regarding the FY24 TSA budget and potential reductions and proposed elimination of certain programs.

- She responded, while not TSA's desire to reduce funding in some of these programs, this decision, along with other budget reductions, has been made because of a cap on TSA's top line budget and the constraints TSA is required to meet. These constraints potentially impact surface, aviation, and some of the technology programs.

Closing

Ms. Fitzmaurice once again personally expressed her appreciation of the Committee's engagement and dedication, and to the partnership and collaboration focused on these important surface transportation efforts. She turned the meeting back to DFO Harroun-Lord.

STSAC Chair and Vice Chair Opening Remarks

Chair Tom Farmer and Vice Chair Polly Hanson offered their sincere appreciation for all assembled and recognized everyone's commitment to the cause of how we function, improve, and collaborate together. They expressed appreciation for all the work that goes into preparing

for these meetings, and emphasized the huge opportunity these meetings offer to highlight challenges and generate fulsome discussions between the Committee and TSA.

Security Risk and Intelligence Subcommittee

The Security Risk and Intelligence (SR&I) Subcommittee Industry Co-Chair and Assistant Chief of Police, Amtrak Police Department James Cook, the SR&I Subcommittee Government Co-Chair Wanda Davis, and the SR&I Subcommittee DFO and Chief of the SISC Darnell Young presented the SR&I Subcommittee update.

Topics discussed included the following:

- The Surface Information Sharing Cell (SISC) membership expansion

- The successfully conducted third classified Industry Day

- The new DHS Homeland Security Information Network (HSIN) SISC page now available 24/7 with an alert feature

- SISC has achieved full operational capability

- The annual DHS compilation of Key Intelligence Questions (KIQs) is due to DHS late June. The SISC will provide an update of detailed Current Industry Information Requirements (CIIR) in conjunction with the DHS KIQ request

Additionally, regarding Recommendation #1, "*Request establishment of a National Intelligence Manager (NIM) for surface transportation,*" progress is ongoing.

- The Subcommittee is working diligently to set the foundation for support of official correspondence from the TSA Administrator asking the Office of the Director of National Intelligence (ODNI) to approve the STSAC's request for appointment of a NIM for Surface Transportation (or similar ODNI advocate) as a security priority. These efforts aim to ensure understanding of what the Committee seeks and why among interested officials at DHS Intelligence and Analysis and at ODNI. The outcome sought is significant and impactful. Effective preparation is essential prior to preparing and submitting the official correspondence.

- The homeland threat environment has significantly shifted in recent years with increased focus on domestic terrorism, cyber threats, and the adversarial activities of nation states like Russia, China, and Iran.

  o This shift demonstrates a need for national intelligence priorities and collection and analysis missions that reflect the heightened volume and variation of cyber and physical threats to surface transportation and critical infrastructure.

  o It also underscores the need for increased and effective collaboration and intelligence and security information sharing among private sector partners, federal, state, and local law enforcement, and the Intelligence Community.

The designation of an ODNI NIM for surface transportation, or a similar ODNI-level advocate, will help advance surface threat intelligence requirements and increase Intelligence Community (IC) analysis and production at an appropriate, and releasable, classification level for sharing with surface and critical infrastructure industry partners with a need to know. This rationale is

similar to NIM-Aviation, whose mission includes advocating for increased collaboration and intelligence sharing with the aviation private sector.

- The NIM-Western Hemisphere (NIM-WH) is the NIM office that may be better poised to serve as an advocate/champion for surface transportation intelligence requirements, as homeland critical infrastructure is in their portfolio. For this reason, TSA is focusing efforts on building relationships with NIM-WH in advance of the formal TSA request for NIM advocacy.

    o The NIM-WH office is currently undergoing changes in leadership and staff, which has delayed arranging the meetings sought. TSA will re-engage with the new NIM-WH leadership and staff to brief them again on TSA intelligence sharing efforts, the SISC mission, and STSAC recommendations.

- In order to advance and fortify TSA efforts to establish relationships with the new NIM-WH, TSA plans to leverage established DHS Chief Intelligence Officer (CINT) partners and NIM-Aviation partnerships.

Next steps for implementing Recommendation #1 include the following:

- Engage with DHS CINT and invite them to join the June meeting to serve as champions for the Surface transportation intelligence requirements.

- Set up an in-person meeting with NIM-WH – with our NIM-Aviation and DHS CINT partners in the meeting to present a unified effort.

- Finalize the memorandum from TSA through DHS CINT to ODNI.

Looking Ahead includes the following:

- The high quality and value of the SISC Industry Days continue to expand and to reach a broader audience.

- With the accompanying growth in interest in participating in the SISC Industry Days, TSA's ability to host in-person classified sessions will likely outgrow available physical-room space. As a result, discussion is warranted on possibility of integrating remote participation in the future.

- The Subcommittee and SISC leadership would consider inviting a value-added, unified industry voice/team to the DHS CINT conversations.

- The SISC is also inviting the DHS CINT and NIM-WH to the SISC Industry Days to provide an opportunity for them to see how information is shared with surface transportation partners.

Insider Threat Subcommittee

The Insider Threat Subcommittee (InT) Industry Co-Chair Chief Joseph Perez, the InT Subcommittee Government Co-Chairs Koi Hallonquist and Lynwood Guise presented the InT Subcommittee update.

Topics discussed included the following:

- The TSA Insider Threat Program is based on the following three drivers:

1. National Insider Threat Task Force (NITTF) minimum standards effected by Executive Order 13587 to assist agencies in developing insider threat programs.

2. The Administrator's 2020 Insider Threat Roadmap.

3. Specific to this group, the STSAC recommendations.

- While the brief is specific to what is going on in the InT Program, it is driven by what TSA is doing to further the STSAC recommendations and transportation security in general.

- Focus areas that align with the Insider Threat recommendations:

1. HSIN Insider Threat Library

2. TSA's Insider Threat Oversight Group (ITOG)

3. Insider Threat Enterprise Case Management System

4. Insider Risk Management Hub (IRMH)

1. The Homeland Security Information Network (HSIN) Surface Transportation Systems Sector (TSS) Insider Threat (InT) Library

- The purpose of the HSIN TSS InT Library is directly in line with the TSA Administrator's 2020 Insider Threat Road Map /Priority 2: Advance Operational Capability/2.2 Establish an enterprise-level, centrally managed capability to integrate, analyze, and respond to potential insider threat information, allowing the Insider Threat program to share perspectives, expertise, and data across multiple offices, agencies, and industry entities, enhancing threat detection, assessment, and response across the TSS.

- The HSIN TSS InT Library has been approved through TSA channels and is moving to DHS HSIN to provision the site within the next three to four weeks. The site will house the Library that holds all the Insider Threat information sharing between industry and government.

- Next steps include establishing a process for soliciting members, determining who will have access, looking at already cleared groups such as PT ISAC, establishing SISC members who should have automatic access, and considering options to directly link all of these sites.

2. TSA Insider Threat Oversight Group

- This interdepartmental group provides oversight and advice to the Administrator and TSA leadership – and will approve operational aspects of the Insider Threat Program, specifically providing legal/privacy guidance.

- Members to date include SES representatives from Chief Counsel and Civil Rights and Liberties, to include the Privacy Office

- The Oversight Group Charter is approved and moving forward through the same three drivers as mentioned earlier.

- While there is no industry participation as such, there is some industry-focused collaboration with the Insider Threat Risk Mitigation Hub (IRMH).

3. The Insider Threat Case Management System (CMS)

- CMS was deployed in November 2022, with about 70 enhancements made to the system since.

- The value of the CMS lies in the potential to analyze trends, provide feedback, and share relevant information instantaneously through the HSIN site in real time. The CMS team is currently collecting data, with attentiveness to trends and patterns in activity, to produce the reports.

- Plans include enhancing local insider threat detection capabilities, as an example, by identifying and tracking patterns from incident reports to be proactive, instead of responding only after an incident has occurred. Local TSA assets will share these findings with transportation stakeholders. This initiative is intended to provide a greater view of what's happening across the nation/transportation sectors.

- The Insider Threat Section continues to collect data to establish a baseline for the CMS's analytics capability. Once a baseline has been established, the Case Optimization and Risk Evaluation (CORE) tool, which runs on top of the CMS, will triage incidents entered into CMS.

- Next steps are focused on thinking very critically and strategically on improvements that will address gaps more quickly and provide analytics to both TSA and industry stakeholders who join.

4. Insider Risk Management Hub (IRMH)

- IRMH members participated in roundtable exercises and testing of incident response plans that were very successful. The IRMH will reach back to the InT Subcommittee to solicit items from the Subcommittee's focus areas for input/best practices. In addition, the IRMH invites members of the full STSAC who are interested in creating a new working group to collect industry best practices/concerns regarding surface vetting – with assistance sought for collaboration on the group's creation. Continued procedural updates and document generation are required to enable maturation of the IRMH and the broader InT Program, which will facilitate mechanisms for incorporating industry representatives.

Next steps for implementing Recommendations #4 and #5 include the following:

- While there have been discussions on recommendations #4 and #5, there are indications that the work slowed pending publication of the NPRM.

- Work has been revived on these to get a sense of what risk-based factors would merit attention.

- Further discussion ensued regarding the vetting rulemaking with a focus on certain sensitive positions.

Highlights include the following:

- Hearty thanks to all who contributed to the standup of the Homeland Security Information Network (HSIN) Surface Transportation Systems Sector (TSS) Insider Threat (InT) Library.

- The Case Management System is exceptional—some from regulations and some voluntary. The team reviews the reports and enters them into the CMS for analysis,

specifically to ensure the reporting meets the intended purposes of informing vigilance and enabling proactive risk mitigation measures.

- Highlighted the recent Air National Guard insider threat incident in which a trove of highly classified documents was posted to social media and discussed the challenges presented by social media in mitigating insider threats. This recent incident underscores the critical importance of insider threat programs and employee education and empowerment. Employees must be trained to recognize the signs of a potential insider threat and they must be provided with the means and opportunity to report their concerns. Co-workers and first line supervisors have a front row seat into what goes on in the workplace. They are uniquely equipped to discern what is normal versus abnormal in their environment, and thereby may be the first to recognize a warning sign. Again, reporting is crucial, and an incident might be prevented if the potential risk indicators are recognized in a timely manner. Everyone is responsible for protecting the transportation system and all have a duty to report.

- Industry echoed the concern and need to expand the approach beyond regulated industries. Insider threat is a top concern.

Emergency Management and Resiliency Subcommittee

The Emergency Management and Resiliency (EM&R) Subcommittee Government Co-Chair Chris McKay and the EM&R DFO Darrin McGreevy presented the EM&R update.

Topics discussed included the following:

- The webinar workshop held in March 2023.

- The Quick Look Report with conclusions that followed.

The EM&R Subcommittee prioritized evaluating the current state of the power grid with the goal of providing relevant information to stakeholders on potential challenges that might arise as surface transportation organizations transition to cleaner technology vehicles and supporting systems. The purposes of the webinar:

1. Provide an overview on the current state of the power grid and deployment of electric and clean technology vehicles in surface transportation modes.

2. Examine the resiliency in sources of electrical power.

3. Identify potential adverse impacts that could result to the surface transportation community in the event of an extended disruption.

Participants included government presenters from the Department of Energy (DOE), Department of Homeland Security (DHS), Surface Transportation Security Advisory Committee (STSAC), and Transportation Security Administration (TSA). Representatives of Pinellas Suncoast Transit Authority (PTSA), Peter Pan Bus Lines, and Duke Energy presented the industry perspective. Around 180 stakeholder invitees attended from Over-the-Road Bus, Pipelines, Freight Rail, Mass Transit, Passenger Rail, Highway Motor Carrier, and private industry associations – plus officials from the Department of Transportation (DOT).

Mr. McGreevy noted the importance of the fact that this workshop served primarily as an information session. Instead of taking actions or making decisions, it afforded the opportunity for participants across the surface modes of transportation hear and learn from industry peers on approaches to this transition and challenges that industry faces going forward.

The presenters noted some interesting facts and observations from the workshop:

Over-the-Road Bus

- The current cost of a diesel motorcoach is about $600,000, or almost half of the cost of an electric motorcoach at about $1.1 million. After purchase and installation, a single charging station for an electric motorcoach can cost upwards of $400,000.

- As a major benefit, electric motorcoaches can cost fifty percent less in maintenance and operate three times more efficiently.

Public Transportation

- One stakeholder intended to increase the number of electric buses from six to 20 by the end of 2023 and to 68 total electric buses by the end of 2024.

- The increase in electric buses would dramatically increase energy usage. Partnering with their local power provider, one stakeholder signed a 10-year agreement to establish electric infrastructure installation, electrical connections, charging stations, and back-up power options in the event of an outage.

Pipelines

- During a power grid disruption, most pipelines would face cascading impacts to support services, response options, and communications. As society moves toward cleaner technology, the electric grid would be responsible for operating pipeline control systems, permitting communications with cell towers, and allowing remote workers to access operations.

- When a disruption to the power grid occurred, adverse impacts affected additional pipeline utilities, such as compressor stations, pump stations, small to medium pipeline facilities, and distributed control systems, all with limited battery back-up available.

Comments about the webinar and possible next steps included the following:

- STSAC leadership attended the webinar and described it as excellent, advocating for more events of this focus and quality.

- The discussion seemed like the beginning of a conversation but was well managed.

- Consider developing another forum to address the many questions and broad interest the webinar generated.

- The current grid might not have the ability to support everyone moving to electric vehicles.

- Some transit agencies produced their own power, which presented new problems.

Commendations, Collaboration, and Looking Ahead included the following:

- Appreciation and thanks were expressed for the representation and demonstration of the public-private partnership in action.

- Exceptional discussion generated on the practicality of transitioning vehicle fleets and the new dependence on the electricity sector that has not existed before. The issue impacted multiple sectors, not just transportation and electricity, but others as well.

- Acknowledgment and appreciation were expressed for the volume of work done here that offers a real opportunity to identify effective practices and help organizations understand what they need to do to prepare for a power grid disruption.

Threat Brief

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

DHS CTC Brief on Physical Threats to Surface Transportation

A DHS Counterterrorism Center analyst provided a brief on Physical Threats to Surface Transportation.

Topics discussed included the following:

- An overview of the terrorism threat to the Homeland.

- Physical threats to critical infrastructure.

- Accelerationism.

- Firearm attacks on electrical infrastructure.

- Threats to the Transportation Sector.

- Recent trends.

There was an opportunity for questions and discussion after the brief:

- Operators must recognize the planning stages before the incident—focus should revolve around identifying these signs and reporting.

- Guides and checklists point to observable indicators and red flags.

- Behavioral approach to violence prevention.

- The SISC previously shared products that have these indicators; Mr. Young will push them to the top of the queue to help understanding.

Cybersecurity Information Sharing Subcommittee

The Cybersecurity Information Sharing (CIS) Subcommittee Industry Co-Chair Norma Krayem and the CIS Subcommittee Government Co-Chair Tim Weston presented the CIS update.

Topics discussed included the following:

- Surface transportation industry's needs for clarification around whether or not the Cybersecurity Information Sharing Act of 2015 (CISA Act) protections convey to an organization when under the requirements of the TSA's Security Directives (SDs).

- Dialogue revolved around protecting information sharing under the CISA Act, addressing legal questions based on voluntarily reporting, sharing incidents across agencies, and how to convey protections and whether or not information reported to CISA pursuant to the SD shifts to exclusive government control for usage and determinations on further sharing by the reporting organization.

- Discussions also focused on ensuring that the CISA Act covers information shared with and through the SISC.

- TSA leadership clarified the agency supports and promotes cyber security information sharing by surface transportation organizations, within their industries as well as across modes, via the SISC, and critical infrastructure sectors. The agency does not intend to review information shared for these purposes as a means of identifying alleged failures to report to CISA in compliance with Security Directives and to seek enforcement action.

Next steps reviewed included the following.

- TSA PPE Surface Division will issue a policy clarification notice on the Security Directives (SDs) issued to pipelines, rail transit systems, and railroads. This notice will make clear that TSA does not review cross-modal and cross-sector information sharing for the purpose of identifying potential failures to comply with the SDs mandates on reporting cybersecurity incidents to CISA. At the same time, the agency does reserve the right to take enforcement action if the circumstances demonstrating a failure to report pursuant to the SD warrant.

- TSA Surface Division Leadership requested that industry stakeholders share their questions in writing so as not to lose anything in translation. TSA would provide the answers in writing.

- The CIS Subcommittee indicated that it has shared a variety of scenarios already with TSA Surface Division Leadership and would prepare an additional list of questions to submit to TSA Surface Division Leadership for policy clarification, if needed.

Committee Administrative Discussion

Committee Vote for the February 16, 2023, Meeting Minutes

Chair Farmer led the Committee vote to accept the February 16, 2023, meeting minutes as distributed to members in advance of the meeting. Mr. Farmer requested a motion to accept the minutes. A Committee member moved to accept the minutes and the motion was seconded by another Committee member. The motion carried by voice vote and the minutes were accepted.

Annual Report for 2021–2022

Chair Farmer discussed the upcoming STSAC Annual Report, thanking everyone for the work reflected in this. Officers, colleagues at TSA, and the committee put the information together to chronicle activity from April 1, 2021, through December 31, 2022. Going forward, the report

will cover Committee activity by calendar year. Draft content will come from quarterly concise reports produced after each meeting to capture progress.

Federal Register Notice

A *Federal Register* notice will be published in June 2023 requesting applications from individuals who are interested in being appointed to serve on the STSAC. With publication, those members who have served their two-year term and members whose term expires in this calendar year should apply in response to this *Federal Register* notice for an appointment if they wish to continue to serve on the Committee.

The Chair and Vice Chair recognized the dedicated commitment of all the volunteers on the Committee, highlighting their accomplishments and urging them to consider another two-year term that would provide further opportunity to put an imprint on the Committee's initiatives. They valued everyone's contributions tremendously and thought it an exciting time for the Committee.

TSA PPE Surface Policy Division Update

The PPE Surface Policy Division Executive Director Scott Gorton presented the Operations Support update.

Topics discussed included the following:

- NPRM for Vetting of Certain Surface Transportation Workers that meets a requirement that Congress mandated in the Implementing Recommendations of the 9/11 Commission Act of 2007.

- Extension of SD Pipeline-2021-01 series.

- Proposed rulemaking for Surface Cyber Risk Management.

Discourse centered around the first topic, the NPRM for Vetting of Certain Surface Transportation Workers.

- *Federal Register* publication of the NPRM is expected within the next seven days; upon publication, TSA will send out a note with a link to access. He urged everyone, and their respective industries, to take this opportunity to provide comments and explanations to let TSA know their thoughts on the proposed requirement and any content and procedural changes they might suggest.

- The NPRM focuses on vetting security-sensitive employees—basically the same population as the Security Training Rule—for freight rail and mass transit modes. These employees would be required to undergo a level two security threat assessment (STA) consisting of terrorism watch list and immigration status checks.

- Those in the designated security coordinator role would undergo a level three STA, adding a criminal history background check to the terrorism watchlist and immigration checks, and following the same process for obtaining a Transportation Worker Identification Card (TWIC).

- The proposed rule also identifies fee structures with opportunities for waivers and appeals, because of the addition of fairly significant populations and the need to have protections in place for them so as not to exclude people from employment.

- The proposed rule should answer questions along the lines of "What does this mean to employers?" and "What happens if an employee doesn't pass?" The preamble and explanation of the processes in the proposed rule discuss these issues in great detail.

- Discussion ensued around fees, vetting timelines, and exemptions.

Next steps included the following:

- The Vice Chair asked for a list of what exempted an individual from the process if they already submitted for a background check such as TWIC, Hazardous Materials Endorsement (HME), PreCheck, Global Entry, FBI background checks or other vetting programs, and those with security clearances.

The continued discourse also addresses the second topic, the Extension of the Security Directive (SD) Pipeline-2021-01 series.

- TSA intends to extend the Security Directive (SD) Pipeline-2021-01 series.

- *Enhancing Pipeline Security*: SD Pipeline 2021-01D will be issued with an expiration date of May 29, 2024.

- SD Pipeline-2021-02C will expire at the end of July 2023. TSA staff considered minor changes based on what has been learned from experience and questions received about cyber-assessment and cyber-implementation plans. A technical roundtable discussion will be held with industry subject matter experts before issuance the new version of the directive. Executive Director Gorton expected the discussion to take place in the next two to three weeks.

Further discussion covered the third topic – the proposed rulemaking Surface Cyber Risk Management.

- The framework and applicability of the rule will be complicated because of TSA's intention to cover pipelines, railroads, and public transportation systems and to establish a structure for cybersecurity programs.

  o TSA intends to use the same format with cyber risk management as was used for the Security Training Rule published in March 2020, namely establishing a security program with component parts.

  o TSA looked at the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), version 2.0, to stay in alignment, resulting in covered parties performing an assessment, creating a plan to monitor, detect, and respond to incidents, all in logical order and leading to complimentary parts of an overall program.

TSA SO Surface Operations Update

Security Operations (SO) Surface Operations (SO) Assistant Administrator (AA) Sonya Proctor provided a Surface Operations update.

Surface Transportation Security Advisory Committee (STSAC)

AA Proctor highlighted good news items of interest to the surface transportation community.

Topics discussed included the following:

- Notice of Funding Opportunities (NOFOs) for the Federal Emergency Management Agency's (FEMA) Transit Security Grant Program, Intercity Bus Security Grant Program, and Intercity Passenger Rail (Amtrak) Grant Program were released on February 27. All three programs had a combined $105 million available, with $2 million for bus, $10 million for Amtrak, and the remainder, $93 million, for transit.

- Gold Standard Awards are a notable accomplishment. The SO team determined the awards based on excellence per the results of a Baseline Assessment for Security Enhancement (BASE) evaluation. Gold Standard Awards have been presented to Southern Nevada Regional Transportation Commission in December 2022, Sacramento Regional Transportation District in January 2023, Jacksonville Regional Transportation District in March 2023, and Niagara Frontier Transportation in April 2023.

- The TSA Administrator has created a unique exercise environment with IBM's "Cyber-range" in the Boston, Massachusetts, area—a new opportunity for those wanting to host exercises on cyber threats, incidents, and response. The range provides a hands-on simulation of breach scenarios. A pipeline company participated in an excellent simulation with TSA, CISA, and FBI observers. Although the pipeline conducts thorough drills regularly, its key personnel cited the value gained with use of the range and realistic scenarios. The IBM range presents an exceptional opportunity to take advantage of an ability to conduct cyber exercises.

- Security Scorecard Tool is a new initiative under which TSA has contracted with a company to enable industry entities to evaluate their internet access points, or external facing internet presence, through a tool running a program to identify vulnerabilities – with scores generated between A to F on exterior presence across six categories of potential vulnerabilities. TSA currently holds 200 licenses and has promoted this capability with the pipeline industry. While not required by security directive, TSA offers this completely voluntary opportunity to request a license and receive it at no cost to do use the tool. A webinar for interested companies will take place on May 18 to explain how the tool worked, featuring a live online demonstration so that attendees can determine whether they would like to participate. This initial webinar has been opened to pipeline companies only by invitation. However, TSA will expand the opportunity to freight rail and aviation next – after pipelines have served as the test group.

- I-STEP exercises present an excellent opportunity, providing a way for surface transportation partners to exercise emergency procedures to ensure their systems remained resilient if affected by some kind of incident, whether physical or cyber. Upcoming events are scheduled in Las Vegas with the Regional Transportation Commission; Brooklyn at the New York Marine Terminal; and a Security Plan workshop in Harrisburg, Pennsylvania, for over-the-road bus stakeholders. During the latter, participants will draft a framework for a security plan to take back to their company to build on and implement, particularly if they did not have one in place previously. Additionally, an active assailant exercise took place on May 15, 2023, in Capitol Heights, Maryland.

- The American Gas Association (AGA) hosted a meeting for Pipeline SD covered companies during which 65 attendees continued ongoing discussions about implementing the SDs. Another meeting took place in Houston in February of this year to talk about cybersecurity implementation plans. Surface Operations staff had reached the inspection stage and some companies that had already completed the process shared what they did to make it smooth and explained what they thought worked well. Events of this kind have continued, and will continue, so that TSA meets the commitment of "no surprises" in oversight and inspections. Communication occurred continually with in-person meetings as companies prepared for a scheduled inspection, helping them understand what to expect, how much time to allocate, what questions inspectors will ask, and what documents are needed. They even knew who would come from TSA, all of which helped make positive experiences during the inspection phase. The next event is anticipated to take place in late summer 2023.

- All the surface transportation systems under the SDs must report covered cybersecurity incidents to CISA Central. Reviews of this reporting has led to the creation of a dedicated CISA report. CISA has reached the point of scrubbing its report to finalize and provide relevant cybersecurity information back to industry. The pipeline industry has reported the longest, since May 2021, generating 1,154 reports, making up 92 percent of everything CISA had received, spread across 45 different operators. The report also contained information about other parts of the transportation system, including aviation, but all of that amounted to just eight percent, or about a hundred incidents. TSA continues to work with CISA to perform a more sophisticated analysis; however, over a third of the cases required follow-up for proper categorization. While the report counted as a start towards analysis, it didn't provide the most helpful level of detail. Industry could alleviate some of that by getting back to CISA with updates.

Chair and Vice Chair Closing Remarks

Chief Hanson shared that she attended Monday's active assailant drill, which the group discussed earlier, found it excellent, and now looked forward to the after action report.

She noted that STSAC leadership built this agenda specifically to hear from participants in industry and government. Everyone should find the meetings valuable and she urged members to provide feedback, suggestions, and comments on what worked and what they would like to hear more about or less of something else. She closed by thanking everyone for coming.

Chair Farmer identified some follow-up actions based on today's discussions:

- Draft annual report.

- Joint representation forming a broader committee to meet with DHS CIRT on appointment of a NIM for surface transportation.

- Applicability of the CISA Act of 2015 to cybersecurity information sharing by surface transportation organizations across transportation modes and critical infrastructure sectors, including through the SISC.

Next steps included the following.

- Continue renewed work on the InT Subcommittee Recommendations 4 and 5.

- Provision the HSIN TSS InT Library site.
- Follow up with interest in further workshops for electric vehicles and the energy sector.

Chair Farmer thanked everyone and the ASAC leadership for joining.

Adjournment

DFO Harroun-Lord asked for a motion to adjourn the meeting. A member motioned to adjourn the meeting. Another member seconded the motion. The motion to adjourn was carried by a voice-vote of the Committee.

The sixteenth meeting of the STSAC meeting was adjourned at 4:33 p.m. EST.

Certification of STSAC May 17, 2023, Meeting Minutes

I hereby certify that this is an accurate record of the activities of the Surface Transportation Security Advisory Committee on May 17, 2023.

Thomas L. Farmer
Surface Transportation Security Advisory Committee Chair