Surface Transportation Security Advisory Committee (STSAC)

Meeting Minutes
August 19, 2021

Meeting Summary

The ninth meeting of the Surface Transportation Security Advisory Committee (STSAC) was held virtually via an operator-assisted teleconference call due to the novel coronavirus (COVID-19) pandemic. The meeting was closed to the public.

Policy, Plans, and Engagement (PPE) Deputy Assistant Administrator (DAA) and STSAC Executive Sponsor, Victoria Newhouse, provided introductory remarks highlighting the renewal of the mask security directive for transportation conveyances and hubs. The Senior Official Performing the Duties (SOPD) of the Deputy Administrator (DADM) Stacey Fitzmaurice provided opening remarks and thanked everyone for their partnership and input. She discussed the mask and pipeline security directives and addressed the current focus on cybersecurity. The STSAC Chair Thomas Farmer and Vice Chair Polly Hanson shared their perspectives on the situation in Afghanistan and the twentieth anniversary of the 9/11 attacks. They introduced the subcommittees' updates on implementation of approved recommendations. Subcommittee presentations focused on the development of implementation plans. The Open Discussion provided all Committee members an opportunity to participate in the conversation. The National Counterterrorism Center (NCTC) provided an Overview of Homeland Terrorism Threat. PPE Surface Policy Division, Executive Director Scott Gorton and Security Operations, Surface Operations (SO) AA Sonya Proctor provided an update on existing TSA Security Directives. TSA Operations Support Acting Executive Assistant Administrator Thomas L. Bush discussed a proposal circulating within TSA to recommend that the Administrator issue Security Directives on cybersecurity for surface transportation modes. The meeting concluded with an administrative discussion, closing remarks from TSA Administrator David Pekoske, and adjournment.

Call to Order

STSAC Designated Federal Officer (DFO), Judith Harroun-Lord, called the meeting to order at 1:08 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 or with connectivity issues. Ms. Harroun-Lord noted a change in the agenda with the switch of speakers for opening and closing remarks due to last minute scheduling conflicts.

STSAC Executive Sponsor Introductory Remarks

STSAC Executive Sponsor, DAA Victoria Newhouse, provided introductory remarks, thanking everyone for their hard work and collaboration. She looked forward to another very important quarterly STSAC teleconference and hoped that everyone continued to stay safe. She mentioned that TSA staff will reassess if they can host the November public meeting in person. Ms.

Newhouse mentioned the determination to renew the mask security directive for transportation conveyances and hubs. The current security directive will expire September 13, 2021; the renewed version will last until January 18, 2022 and may possibly extend beyond that date depending on Centers for Disease Control (CDC) assessment. TSA will post the finalized directive and share it with STSAC committee members following CDC guidance. Ms. Newhouse concluded by thanking attendees for their support and input on many different areas. She then turned the meeting over to Ms. Fitzmaurice.

Senior Official Performing Duties (SOPD) of the Deputy Administrator Opening Remarks

SOPD DADM Fitzmaurice provided opening remarks. She started by welcoming everyone. Ms. Fitzmaurice was pleased to kick off this event. She thanked everyone for their partnership and inputs that have proven extremely valuable to TSA and the public at large. She gave a special salute to Chief Ronald Pavlik, who intended to retire from the Washington D.C. Metro system on September 21, 2021, and accepted a position for the Deputy AA for Surface Operations (SO), which he would assume after that date. Ms. Fitzmaurice anticipated Chief Pavlik would become a tremendous asset as a TSA employee.

Ms. Fitzmaurice thanked the committee members for their annual report and eighteen recommendations, which would allow for continued improvement and safeguarding of the nation's transportation systems. TSA reviewed and concurred with them all and provided concurrence and the STSAC's annual report to Congress. Now, the focus turns to implementing the recommendations. She thanked the subcommittees, with those outside and inside TSA working to develop implementation plans. She committed TSA to transparency on this; part of that would include publishing quarterly progress reports.

TSA followed the science when issuing the mask security directives. Her staff worked closely with CDC as cases rose, particularly with the variants, and agreed that mask wearing in public transportation venues would help minimize the spread. Ms. Fitzmaurice thanked everyone for all their continued support of this requirement.

Issues and challenges have continued unabated over recent months. Ms. Fitzmaurice believed cybersecurity rose to the forefront of those, and she expected good discussion during the meeting on that topic. She mentioned the issuance of two security directives within the pipeline mode to strengthen cybersecurity on the nation's most critical systems. TSA staff completed work on these based on very specific information and threats. She appreciated the conversations that have taken place so far on their implementation because she knew the security directives presented a heavy lift for companies and required close collaboration and partnerships with the Cybersecurity and Infrastructure Security Agency (CISA) and many others within the transportation system. She extended her appreciation to include federal partner support as TSA continued to move out on these efforts. She urged everyone not to lose sight of the fact that the threat encompassed more than just pipelines, and they ultimately needed to prepare to keep attacks down on all modes of transportation, including aviation. In light of this, some offices have started to grow their cybersecurity capabilities. TSA expects to have a Cyber Support Branch with about 10 personnel in place by the end of September. The Surface Policy Division had also increased their efforts and expected to expand positions from six to nine. Out in the field, inspectors have received very specific cybersecurity training to help them implement the best practices and guidance so that the surface transportation system remained resilient with

cybersecurity built in throughout. Ms. Fitzmaurice concluded by pointing to the busy agenda for the meeting. She appreciated her chance to provide opening comments.

Subcommittees Updates on Implementation of Approved Recommendations

Mr. Farmer kicked off this part of the agenda by thanking everyone for giving him the opportunity to serve as the STSAC Chair. The committee members have provided tremendous support and work effectively. He felt privileged to play a part in it. He called attention to the large amount of progress made since the last meeting, especially when it came to implementing all the subcommittees' recommendations and praised everyone's excellent efforts. He gave particular commendation to the Ms. Harroun-Lord and to Ms. Felicia Archer, Program Analyst, Surface Policy, who provided support to the overall effort across the subcommittees. Mr. Farmer recognized that this work came in addition to other demands that have persisted for a long time, such as the pandemic, hurricane season, and disruptive acts of violence stemming from earlier protests. He thanked industry and government personnel for their commitment.

Chair Farmer saw a stark reminder about the importance of their work in the situation in Afghanistan in the wake of the Taliban's seizure of power and the prospect of Al Qaeda and other terrorist groups finding a sanctuary to reconstitute and increase power. He viewed with alarm the ongoing evacuation challenges as he suspected an intensified terrorist threat stemming from the power vacuum. Historically, intelligence analyses have shown that terrorist groups like Al Qaeda and ISIS have expanded their capabilities and reach to execute attacks in Europe and beyond after obtaining safe havens. The STSAC's recommendations have placed a strong emphasis on advancing proactive capabilities, procedures, and measures for sustained preparedness to identify threats, detect indicators of concern, and report to deter terrorist-related activity.

Bringing it closer to home, the STSAC will update TSA senior staff monthly on progress with the subcommittees and implementing the recommendations. If challenges are encountered, the Committee will act to align support, resources, and tools to resolve these matters. Chair Farmer expressed the aim that updates convey a good understanding of progress attained and clear thoughts on how to resolve impediments.

Vice Chair Hanson highlighted what has happened since the May 20, 2021, meeting: Administrator Pekoske returned to TSA. Ms. Hanson urged everyone to keep in mind the twentieth anniversary of 9/11 attacks, which provided the reason for the STSAC's existence, as well as their work and the tools they use to accomplish it. She looked forward to hearing the subcommittees' reports. She expected the presentations to answer, "What worked well? What do we need to resolve challenges?" She also pointed ahead to the agenda item that gave the chance for open discussion. Then she thanked everyone for their service and turned the proceedings back to Ms. Harroun-Lord.

Security Risk and Intelligence Subcommittee

Mr. John Beattie, subcommittee government co-chair, turned to Mr. Darnell Young, as the latter had done the lion's share of the work. Mr. Young introduced himself as Chief of the Surface Information Sharing Cell (SISC) and the DFO for this subcommittee; then expressed his thanks

for the support from government agencies and industry partners. His subcommittee made four recommendations, which he walked through individually.

1. Establish a National Intelligence Manager for surface transportation: The subcommittee had prepared a document for release on August 25, 2021, in which they leveraged their expertise. They would also provide additional feedback to the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) to express industry concerns. Mr. Young viewed their first recommendation as having long-term strategic value and also potential short-term gains. While the subcommittee originally planned to send the second document to DHS and ODNI by the end of September, they have pushed that deadline back to allow industry leaders time to comment.

2. Use private sector intelligence requirements to guide federal intelligence collection and inform intelligence analyses and product development by Intelligence Community agencies and analytical centers: Tremendous support emerged from industry counterparts for this recommendation. The subcommittee put together industry requirements on June 17, 2021. TSA staff reviewed those against existing requirements on July 28, 2021, to determine overlap. Additional requirements can go out to other government agencies to address as necessary. They will ultimately receive and provide feedback to their industry partners.

3. Approve and implement the SISC charter: Industry and government subject-matter experts have provided tremendous support, working on drafting the SISC charter during twice weekly meetings. In between those meetings, they moved the process along with emails, phone calls, and participation from TSA's Chief Counsel to complete the charter. They have forwarded it for next phase its of development, convening separately over the past week to discuss the charter in preparation for an August 25 meeting. ODNI, DHS, CISA, TSA, STSAC elected officers, and industry members all supported the effort.

4. Complete the Security Risk Methodology Matrix as a resource to support efforts to drive down risk across surface transportation modes: The subcommittee views this recommendation as long-term. Ultimately, they will build out thirteen risk models, but right now they have picked one to use as a sample and solicit input from industry. Then they will attack the remaining twelve. Mr. Young estimated they would finish the example by the end of summer plus an additional month to solicit feedback. Finally, they will collect, compile, and submit all of them to the TSA Administrator.

Mr. Young cited time as the biggest challenge. The subcommittee mitigated that with their biweekly meetings. He identified additional support as necessary going forward to push through the recommendations. To keep everything moving, he urged everyone to pay attention to their inboxes and respond in a timely manner or notify him if they could not. The subcommittee would take more help from anyone if they had interest.

Cybersecurity Information Sharing Subcommittee

Mr. Timothy Weston, subcommittee government co-chair, wished everyone a good afternoon. He thought it fitting that he followed Mr. Young's updates due to their close collaboration. He then recapped his subcommittee's four recommendations.

1. Establish a surface transportation cyber information sharing network on threats, incidents, and security concerns and related alerts, advisories, analyses, and assessments: Work had begun to establish the network and coordination continued with TSA Intelligence & Analysis

(I&A) and CISA on information sharing. They captured reporting requirements in their charter and would follow that with implementation plan development, plus conduct additional outreach with stakeholders on specific communication links to share information. Subcommittee members anticipated handling this more specifically in the implementation sharing phase.

2. Manage the operations of the SISC under the express authorization provided by the Cybersecurity Information Sharing Act of 2015: The subcommittee established a working group with TSA Chief Counsel and DHS General Counsel representatives for this specific recommendation. They still plan to do more since the pipeline security directive requirements to share information took the forefront. They will decide on how to use the Cybersecurity Information Sharing Act of 2015 moving forward, as they want to integrate that into SISC operations and included it specifically in the SISC charter. Mr. Weston stated that it met a big part of the need there.

3. Establish effective procedures for broad sharing of cyber threat and security information across surface transportation modes: The subcommittee tied this recommendation directly to SISC operations, capturing its intent. They need to do further work on implementation.

4. Conduct an annual review to assess the performance and impact of the SISC: The subcommittee will also incorporate this into the SISC charter. Work has begun with DFO Young to do so. Once fully operational, they will consider it complete.

The subcommittee has hosted field intelligence meetings with cyber teams and continued to work with CISA to meet recommendations. They have focused most of their efforts on the charter through a specially dedicated work group. The industry co-chair position has fallen vacant, which posed a problem, however they have undertaken efforts to fill it. A co-chair will join soon, and then they can consider themselves as completely staffed. Mr. Weston also looked forward to the SISC becoming fully operational.

Mr. Lee Allen, subcommittee DFO, thanked Mr. Weston for his report which summarized everything well. He also wanted to mention his work with the SISC on Memorandums of Understanding (MOUs)/Memorandums of Agreement (MDAs), now formulated and approved so that they could proceed with their information sharing requirements.

Insider Threat Subcommittee

Colonel (Ret) Michael Licata, subcommittee industry co-chair, introduced himself as the private sector co-chair for the Insider Threat Subcommittee. He had established a great working relationship with TSA's government co-chair, Mr. Matthew Hudren. Mr. Hudren's diligent engagement with the subcommittee achieved agency buy-in, secured funding, and brought MITRE onboard to begin work. Mr. Hudren had a full plate with TSA insider threat initiatives and coordinating with the aviation program. Colonel (Ret) Licata thought the workload would benefit from additional resources, at least one other person at a minimum.

Mr. Hudren expressed his appreciation for Colonel (Ret) Licata's comments. He introduced himself as TSA's Section Chief for Insider Threat. The Insider Threat Subcommittee had made significant progress with their recommendations. He addressed each recommendation strategically and referred to a briefing later on the agenda to talk about domestic and homegrown violent extremism. He had considered this a priority for a number of years, along with making

an exception to break out of a modal focus and look across all sectors to mitigate threats. He reported that they had not seen much, nor had they unearthed anything relevant or critical, yet they would not let down their guard and would continue to search for things. They had also brought in other federal partners to help address two areas.

1. First, they established professional insider threat hubs. MITRE employed their expertise to decide what to do better and make the program more holistically sound by working on a recommendation paper. The hubs require funding. To help with this, Mr. Hudren brought unfunded proposals and unfunded requests up to do date. Currently, MITRE had reached out to Mr. Joe DeLuca and Colonel (Ret) Licata to facilitate including the aviation security aspect and incorporating that mode's perspective – because the Aviation Security Advisory Committee (ASAC) plays a substantial part in TSA's program. He hoped to secure funding in year five years to create a better environment and had success with two unfunded requests recently funded. They need to incorporate all methodologies that TSA uses at the enterprise level. The effort to incorporate all analytic methodologies across the enterprise will come together with the Case Optimization and Risk Evaluation (CORE) tool that will align all databases in one place to facilitate study of them. From there, they examine the risk by asking, "What's pertinent to TSA, to surface, to aviation?" While they know some of this already, the CORE tool would better enable them to mitigate unseen threats. Mr. Hudren expected these projects to take a year or two, as they would build out all this in Salesforce. They had brought in aviation and surface transportation partners to make the tool work and avoid any gaps. They wanted this tool to last a long time while proving productive and applicable to the whole community.

2. Mr. Hudren referenced progress to analyze risks and threats with tools to cover their other recommendations, particularly an Insider Threat Steering Committee. Everyone plays an important part, whether commercial aviation, TSA, or surface transportation. The subcommittee explored having the newly formed steering committee sit together with the Director of the Federal Air Marshal Service or bring in members individually to offer ideas and objectives as part of the solution to make everything work. Those meetings would take place quarterly or semiannually, and participants would propose updates at that time.

Mr. Hudren had received lots of help and support with all these initiatives and programs. However, he had still experienced challenges, particularly with resource constraints, as his insider threat environment and duties had broadened substantially. He viewed STSAC as a big help. DFO Harroun-Lord had given tremendous support as she kept things up-to-date and informed leadership. Ms. Archer had assisted the subcommittee in their endeavors, and her actions had definitely made a great contribution, enabling them to move forward. He concluded by thanking everyone else.

Emergency Management and Resiliency Subcommittee

Ms. Jennifer Gibson subcommittee industry co-chair thanked the attendees for the opportunity to provide an update on the subcommittee's progress. She specifically addressed the subcommittee's two recommendations.

1. Enhance pandemic preparedness by sharing lessons learned on response to COVID-19 across modes: The subcommittee had accomplished this priority by disseminating the report developed from the September 2020 best practices and lessons learned workshop, posting this on respective government websites and in resources maintained by TSA and the

Department of Transportation (DOT) where applicable. The subcommittee is also in the process of reaching out to academic institutions with emergency management programs to provide the report to incorporate into their curriculum. To date, the subcommittee had succeeded in verifying the report's posting to appropriate places and anticipated completing the sharing of the report with academic institutions by September 30, 2021.

2. Support COVID-19 continuing education to enhance response capabilities and resiliency through recurring review and update of the report on effective practices and lessons learned and supporting information: With the surges of confirmed cases nationally, responses by surface transportation organizations improved based on previous lessons learned. The subcommittee is planning to hold a follow-up COVID-19 workshop to further learning and meet three objectives: 1) identify challenges to restoring full service, 2) discuss protocols for vaccinated/unvaccinated passengers, and 3) determine measures to prepare for the next pandemic. Ms. Gibson identified the target date for holding this as sometime in December 2021.

Ms. Gibson cited the most significant challenge for the subcommittee as securing contractor support for the second workshop, as they had it in place for the first one. She felt cautiously optimistic that they could accomplish this. She knew they have more to learn.

Open Discussion: STSAC Innovation

Ms. Harroun-Lord opened this part of the meeting by asking attendees to answer the question, "What are we missing?" She expected a full and open discussion and thanked everyone in advance for their participation.

Chair Farmer explained the purpose of this segment to the assembled group. He recalled how typical STSAC gatherings had focused recently on subcommittee reports and the work they have done, which he found exceptional. However, when agendas concentrated only on those efforts, others might not have received opportunities to suggest additional areas that needed attention or STSAC members could raise ideas for how to progress better. Mr. Farmer urged everyone to participate; both voting and nonvoting representatives could bring items forward. The assembled expertise in the committee renders vital assuring the opportunity for all to contribute in proposing, shaping, or defining priorities for the continued collaborative effort. He particularly emphasized the value of thoughts on innovation in the focus and substance of the Committee's work. The STSAC could redirect their efforts, if necessary, to address these.

Ms. Hanson echoed the anticipation of the value from hearing the full Committee input, opening it up for participants to make suggestions by asking, "Where are the gaps?" Ms. Harroun-Lord thought that everyone could speak at will during this portion of the meeting. She verified the technical capabilities with the operator. The operator explained that all Committee members had open and interactive lines, needing to unmute themselves on their own phones. Executive Director Gorton also encouraged people to speak.

Ms. Phifer introduced herself as a representative of the American Association of State Highway and Transportation Officials (AASHTO). She viewed highway bridges as very accessible to the public. She urged everyone to visualize an important, iconic bridge; she considered iconic bridges as key facilities with open vehicular traffic and sometimes even pedestrians as well. She wondered if current laws and regulations might not reflect the risks for those using them. Some

have signs posted for those who do not have proper permission to access the structure. She asked for a review of what rules and laws apply so that they can use the best of those and try to move them forward when encountering trespassers.

Mr. Farmer asked Ms. Phifer a follow-up question. As he understood it, she looked to consolidate resources at state and local levels into a reference source so those with responsibility for securing the bridges could understand the lay of the land and their options for trespassers. He agreed this might prove beneficial if they collected it all in one place. A bridge in another geographic jurisdiction might not have as stringent of rules, so local laws would need revision.

Ms. Phifer knew of many rules covering key facilities. She wanted to look at them from the highway point of view. Then they could strengthen their posture in that mode.

Chair Farmer thanked her for this thought. Then he urged others to contribute their ideas. After a period of silence, he raised one himself, something he noted had received lots of attention since the major pipeline incident. He thought that providing the opportunity for the STSAC to develop some form of strategic concept for cooperative effort to elevate cybersecurity practices and help prevent any reactive posture to take action in response to an incident would help achieve consistency on recommended approaches from industry, which could then adopt and adapt them to enhance their performance. He had already held a discussion with TSA's Ms. Sonya Proctor, Assistant Administrator of Surface Operations, on trying to produce this concept and stated his intention to put together a draft explaining the process that week. He would focus on cybersecurity information sharing to manage risk, which might count as another area for consideration. This initiative would build on work the STSAC had already undertaken. He thought that leveraging recommended approaches across organizations could narrow their risk profile. Mr. Farmer promised to develop his document further and provide it for Committee members' review and comment. Then they could decide whether or not to pursue it.

When no one else had anything further to contribute, Chair Farmer stated his intention to make this open discussion opportunity a recurring agenda item. That way, members could organize their thoughts to present to the group in advance. Ms. Harroun-Lord took this opportunity welcome to Steve Alterman, the Aviation Security Advisory Committee (ASAC) Chair. She then introduced the National Counterterrorism Center (NCTC) team for their presentation on two topics with three speakers.

Domestic Terrorism Information Brief

The National Counterterrorism Center (NCTC) provided an overview of the terrorism threat posed by homegrown violent extremists (HVEs) and domestic violent extremists (DVEs), with discussion afterward.

Mr. Farmer summarized the questions/concerns as falling into two categories. The first revolved around threats at the southern border. The second concerned indicators that they could link to violent demonstrations, particularly those behaviors or attire that might serve as warnings.

NCTC offered to organize a separate briefing for this. In the meantime, NCTC highlighted a product, *HVE Mobilization Indicators (2019 Edition)*, which covers this topic in more detail by describing the indicators of progression from radicalization to violence.

Mr. Farmer and Ms. Harroun-Lord thanked the NCTC team. Mr. Harroun-Lord closed this part of the meeting by expressing her appreciation for the partnership in developing the briefs.

TSA Security Directives Update

Executive Director Gorton kicked off the discussion with information on the recent security directives. TSA shared the two pipeline security directives (SDs) with the STSAC members. TSA issued the first pipeline SD on May 26, 2021, which required the appointment of a cybersecurity coordinator, reporting of cybersecurity incidents to CISA, and a self-assessment benchmarked against existing pipeline guidelines. TSA issued the second pipeline SD on July 26. The Transportation Security Oversight Board (TSOB) has since ratified them both, meaning that they met legal requirement to be in effect for more than ninety days. TSA had consulted with CISA and other federal partners with equities in pipeline safety/security and collected significant feedback from industry when writing the directives. Substantial effort was devoted to incorporating those comments, particularly with extending time periods for implementing mitigation measures. A series of questions on implementation of the mandated actions and measures has ensued. Mr. Gorton recognized that companies viewed implementation as a major undertaking, requiring extra labor hours and capital investments to make everything happen. However, TSA had seen a willingness to comply.

Queries continued to come in to clarify the scope and intent so that owners and operators could do just that. TSA Surface Policy has issued a set of Frequently Asked Questions earlier that week and would build upon those. Responding to individual operators would take some time. Some have posed complicated questions, particularly when asking about specific items in their Information Technology (IT) and Operational Technology systems. Those systems have some commonalities, yet all operations are somewhat different. Mr. Gorton thought approaching each of the pipelines individually would be the best and most useful plan. Ultimately, they would meet the goal to have critical pipeline systems put measures in place to continue operations even if subject to an attack.

The second security directive had three sets of required actions: 1) specific mitigation measures to reduce risk of cyber-attack, 2) development of a cybersecurity contingency plan to assure resiliency and limit degradation of operations, and 3) testing of the effectiveness of cybersecurity practices through a cybersecurity architecture design review, which should resemble the Validated Architectural Design Review (VADR) that DHS/TSA had conducted already on a number of systems to identify potential vulnerabilities. Mr. Gorton introduced Ms. Proctor to talk about compliance with the first security directive, now in effect for a couple months, and then she would discuss the plans for the second security directive.

Ms. Proctor thanked Mr. Gorton and condensed her remarks to make up some time. She appreciated the STSAC Chair and Vice Chair sharing their strategic concept on cybersecurity in the Transportation Systems Sector. She viewed this proposal as an important issue to look into when launching detailed cybersecurity initiatives within surface transportation. Following up on the previous presentation, the first pipeline SD had three requirements and went into effect on May 28. Her staff had verified one-hundred percent compliance from all affected parties in submitting self-assessments, appointing their cybersecurity coordinators, and fulfilling their obligation to report cybersecurity incidents to CISA. The second security directive became

effective on July 26. The first due date had not hit yet, so those affected companies still remained in the preparation period, doing work to ensure compliance. They have complied with notifying TSA of their receipt of the security directives and affirming their cybersecurity coordinators. Based on discussions with industry, Ms. Proctor expected one-hundred percent compliance by the first due date. She knew that pipeline stakeholders had lots of questions about the scoping of the security directives, yet those did not stop them from complying with the first one and she expected the same for the second.

Because the second pipeline SD is more complex, TSA Surface has set up provisions for companies to submit a request for consideration for alternative measures if they believe that appropriate. TSA then has to approve those, which Ms. Proctor viewed as a different environment from the type of work the agency had done before. She made it a priority for responses to go out in a timely way. The credentialed Transportation Security Inspectors (TSIs)—whose positions were formed two years ago and who have received CISA training—will deploy in the field for compliance and enforcement issues. The security directive remains in place for one year—these TSIs plan to visit every regulated company over the next year. They would coordinate and announce their visits and work collaboratively to review paperwork and answer any questions when they arrived.

TSA continued to work very closely with CISA for the cybersecurity expertise needed for issues and would tap that agency as necessary. With the second security directive still in early processes, as they move through due dates, the TSIs will do a review of intake procedures and follow up with companies as needed based on their submissions. TSA had a twenty-year history of working collaboratively with the pipeline industry. Ms. Proctor wanted to ensure that her staff understood the new requirements while continuing to perform all other initiatives—such as exercises, information sharing, and responding to needs to comply with these directives—with the same collaborative spirit. She anticipated giving another update in November, as the second security directive's first due date will have passed by then. She then turned the meeting back over to Mr. Gorton and Ms. Harroun-Lord.

Mr. Gorton paused to see if anyone had questions. Hearing none, Ms. Harroun-Lord introduced Mr. Thomas L. Bush, Executive Assistant Administrator, TSA Operations Support.

Operations Support Update

Mr. Bush thanked Mr. Gorton and Ms. Proctor for discussing the pipeline security directives (SDs) and turned to the broader cybersecurity topic. The Administrator had asked for next steps on incorporating actions from the first pipeline SD and certain aspects from the second pipeline SD into cybersecurity SDs and ICs, moving them across a larger group of surface industries and eventually into the aviation side. TSA would focus on surface transportation cybersecurity first and work to implement the same four actions for the rest of the surface industries, including: 1) cyber point of contact, 2) requirement to report incidents to CISA, 3) self-assessments on cybersecurity practices through information circulars, as opposed to security directives, and 4) contingency plans for service interruptions/shutdowns. Although many operators had contingency plans in place, these plans now needed to include cyber considerations. The Administrator has requested a proposal of how best to implement these actions, likely with a combination of Security Directive and Information Circulars. Mr. Bush paused at this point for questions/comments.

Chair Farmer appreciated the update. The STSAC had a proposal for the Administrator's consideration, similar to what Mr. Bush had described. Mr. Farmer understood the intent to apply the cybersecurity provisions across all modes and wanted to do so while remaining consistent with the public private partnership TSA and industry had developed over the past twenty years. He asked for consideration of this document as it outlines areas of emphasis, incorporates some of the other security directives, and implements a roadmap.

Mr. Bush agreed. He promised to raise the topic with the Administrator and also would check with Mr. Gorton and Ms. Proctor so that they could work this into the Administrator's decision-making process.

Mr. Farmer thanked him for his consideration.

Ms. Harroun-Lord asked if anyone else had any questions. Hearing none, she moved the meeting on to the administrative discussion agenda item.

Committee Administrative Discussion

Ms. Harroun-Lord explained how TSA had received 24 applications for open STSAC positions in response the Federal Register announcement. Staff are now in the process of reviewing them.

Initially, there was a small number of submissions, however, a rush occurred in the last few days. Those who applied represented a large pool of expertise. The Committee is mandated to not exceed forty members. The STSAC had five vacancies to fill. Subsequently, TSA will establish a selection team to evaluate the applicants and provide recommendations to the Administrator of the most appropriate people based on an evaluation process assessing their skillsets and the groups they represent. The board would use the same criteria as when the STSAC was initially stood up.

Mr. Gorton thought it good news to have so much interest including from leaders in cybersecurity. His staff intended to complete the selection process and laid out a plan to have the individuals identified and ready to go by the next meeting in November. He promised to move out smartly. People continued working on it daily and would push to make sure they could complete the evaluation and selection process in a timely fashion. He summarized his remarks happy with the good news about so many people expressing an interest in serving.

Vote to Accept May 20, 2021, Meeting Minutes

Chair Farmer instructed members of the Committee of the need to take action on the May 20 Meeting Minutes. A Pre-Vote Copy of the May 20 Meeting Minutes was distributed in advance to Committee members. Mr. Farmer requested a motion to accept the May 20, 2021, Meeting Minutes. Mr. Smith moved to accept the minutes and the motion was seconded by Mr. Finnegan. The motion carried by voice vote and the minutes were accepted.

Chair and Vice Chair Closing Remarks

Chair Farmer stated that he had already spoken often and would let Vice Chair Hanson go first. Vice Chair Hanson enjoyed the subcommittee briefings. She thought the NCTC had given an informative and valuable presentation which generated good dialogue afterwards. She returned to the 9/11 theme she mentioned earlier and recalled how at that time, all across the country, people vowed to never forget. The nation emerged from that period more resolved to protect our freedoms. None of today's participants would ever forget the attacks nor those who lost their lives. She predicted the same would hold true for Afghanistan. Terrorism remains an evil that still exists in our world today. Ms. Hanson thanked to everyone, friends and fellow STSAC members, for continuing to fight to secure surface transportation. She concluded by urging everyone to stay safe.

Mr. Farmer found these remarks very poignant. He also wanted to express his sincere appreciation for the subcommittee reports. The presenters addressed each area very well where they had made progress since the last meeting and also highlighted their impediments. He felt glad that they found support, particularly from DFO Harroun-Lord and Ms. Archer.

Ms. Harroun-Lord thanked both the Chair and the Vice Chair, and then introduced those making closing remarks.

TSA Administrator Closing Remarks

Administrator Pekoske offered to close the meeting. He expressed appreciation everyone's work and felt pleased with how the STSAC had developed. He called attention to the work from the subcommittees, the Chairs, and all the volunteer efforts from the members and government personnel. The Administrator noted his goal to have two advisory committees that steer the agency in substantive ways, and that they had achieved this. For instance, April's report included eighteen great recommendations. TSA responded to them, sending the report to the Hill. Administrator Pekoske thought this reflected significant effort from a committee that had only recently stood up.

He wanted to highlight the cybersecurity threat and knew today's participants had talked about the two security directives issued to certain companies within the pipeline sector. TSA made the first one very public. The second contained Sensitive Security Information (SSI), which limits distribution and access and precludes adversaries from gaining awareness of the detailed measures prescribed. The Administrator expected that the cybersecurity focus would continue in aviation and other surface modes.

The Administrator also thought it important that TSA and DOT continue to carefully coordinate their work, as they had done for the last twenty years. TSA came out of DOT, which helped, as they enjoyed bedrock relationships from the beginning, and he wanted this to continue. He viewed safety and security as two sides of the same coin. Safety and security concerns also reinforced each other, so the federal government needed to coordinate their approach for both. He felt happy with the relationship right now and expected it to evolve and strengthen. TSA staff also worked closely with CISA, a relatively new—only three years old—and rapidly growing agency. Administrator Pekoske made it a goal to have CISA serve as the focal point for all things cybersecurity, except for when it came to the military and .mil email addresses. He assured the STSAC members that it was very intentional that the security directives required informing CISA of significant cyber incidents, not TSA. Doing so reinforced CISA's role and

gave industry a single point for reporting. TSA received these reports in near real time. CISA also had responsibility for critical infrastructure security, so the Administrator identified this as another reason for ensuring they took the lead.

Administrator Pekoske looked forward to continuing to work with the STSAC. If the agencies collaborate and the committees do their work well, that will make things much more coordinated and logical for those outside of government looking in. The Administrator assured everyone that TSA staff would maintain cooperative efforts as strongly as they always had with other industry and government partners. The FBI Director and others have expressed concerns about an increase in domestic terrorism threat in the U.S., so his agency continued to bake in changing profiles into their risk assessments and let those drive activities. He urged everyone else to stay mindful of this. The new threat vector concerned him because of it difference from foreign terrorists or those acting due to foreign influences and changed how TSA could respond.

He viewed Ms. Proctor and Mr. Gorton as two great leaders and appreciated them. He felt privileged to have Chief Pavlik also joining TSA to further strengthen an already very strong team. Congress passed new legislation to direct hire cyber-professionals, enabling a relative rapid onboarding process for them. The Administrator wanted that expertise resident in his agency and in other sector risk management or subsector specific agencies, plus within the Department of Defense (DoD), so that it did not collect all in one spot. He knew they did not have enough cybersecurity professionals, and everyone had to work very hard to bring them onboard.

Administrator Pekoske ended his remarks by expressing his appreciation for all the work done and looked forward to continuing their collaboration. DFO Harroun-Lord and Ms. Newhouse did a great job, as well as the STSAC Chair and Vice Chair. He thanked everyone for all their work.

STSAC Executive Sponsor Closing Remarks

Ms. Newhouse named the team and thanked them individually. With the twentieth anniversary of the terrorist attacks of September 11, 2001, nearing, she commended the efforts of those who had worked tirelessly and selflessly to build a new agency and to develop and expand and enhance its partnerships across transportation modes. She emphasized this "Service" and its importance and how it continues, whether in the form of physical or cyber security or rescuing those in harm's way in Afghanistan. She recalled getting out of the Pentagon on 9/11 and wondering what came next. The efforts of those assembled in this Committee, and in the Aviation Security Advisory Committee, have made what came next work.

Ms. Harroun-Lord thanked both the Administrator and Ms. Newhouse, and then the Committee and all participants.

Adjournment

DFO Harroun-Lord sought a motion to adjourn the meeting. Ms. Natalie Jones-Best motioned to adjourn the meeting. Ms. Eileen Phifer seconded the motion. The motion to adjourn was carried by a voice-vote of the Committee. The ninth meeting of the STSAC meeting was adjourned at 3:55 p.m. EST.

Certification of STSAC August 19, 2021, Meeting Minutes

I hereby certify that is an accurate record of the activities of the Surface Transportation Security Advisory Committee on August 19, 2021.

_____

Thomas L. Farmer
Surface Transportation Security Advisory Committee Chair