# Surface Transportation Security Advisory Committee (STSAC)

**Meeting Minutes**

**May 20, 2021**

## Meeting Summary

The eighth 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.

Acting Deputy Secretary of Homeland Security David Pekoske; TSA Senior Official Performing the Duties (SOPD) of the Administrator Darby LaJoye; STSAC Executive Sponsor Victoria Newhouse, Policy, Plans, and Engagement (PPE); Surface Division Executive Director, Scott Gorton, PPE; and the STSAC Chair Thomas Farmer and Vice Chair Polly Hanson addressed the Committee.

## Call to Order

The STSAC Designated Federal Officer (DFO) Judith Harroun-Lord called the meeting to order at 1:04 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. DFO Harroun-Lord acknowledged TSA leaders from across the enterprise who had joined the call.

## STSAC Executive Sponsor Introductory Remarks

STSAC Executive Sponsor Victoria Newhouse (PPE Deputy Assistant Administrator) provided introductory remarks.

Ms. Newhouse thanked DFO Harroun-Lord and welcomed everyone to the meeting. She acknowledged the outstanding work performed by the Committee in order to submit 18 recommendations to the TSA Administrator. Ms. Newhouse also expressed her appreciation to Acting Deputy Secretary of Homeland Security David Pekoske for providing opening remarks for today's meeting and to TSA Senior Official Performing the Duties (SOPD) of the Administrator Darby LaJoye for providing closing remarks. She recognized the industry partners, federal partners and top TSA leaders, including Executive Assistant Administrators and Assistant Administrators who joined the call today. She remarked that STSAC recommendations and implementation plans are supported by our senior TSA leaders.

## Acting Deputy Secretary of Homeland Security Opening Remarks

Acting Deputy Secretary of Homeland Security David Pekoske provided opening remarks.

Mr. Pekoske explained that he was working out of the Department of Homeland Security's (DHS) St. Elizabeth's campus performing Deputy Secretary duties while new political appointments are going through the confirmation process. Mr. Pekoske expects to be back at his permanent position in TSA by July.

Mr. Pekoske expressed his appreciation for everyone volunteering their time and expertise to help secure the Nation's surface transportation systems. He was delighted with the STSAC Chair and Vice Chair, as they've done a tremendous job in standing up the Committee. He further elaborated on the significant accomplishments and notable advice from industry Committee members in the process.

Mr. Pekoske recently met with the STSAC Chair and Vice Chair to discuss STSAC updates and the submission of the 2020 STSAC Annual Report. Everyone, including Secretary Mayorkas, appreciated these contributions. Mr. Pekoske concurred with all 18 recommendations made and advised the Committee that TSA will provide a formal written response to the STSAC addressing the recommendations and implementation planning within the statutory 90-day timeframe.

Mr. Pekoske particularly appreciated the hard work of the four subcommittees and their working groups for the remarkable progress that has been made.

Mr. Pekoske discussed the threat landscape to the homeland and surface transportation modes, highlighting domestic terrorism. While TSA's threat focus has been on the foreign terrorist threat, the U.S. government is aware of domestic terrorist concerns. This threat vector is particularly concerning because domestic terrorists tend to act impulsively and often alone. Subsequently, it is notable that domestic terrorism might be more of a threat to surface transportation venues than to aviation because of aviation's more visible security envelope. Prevalent analyses in cases across the country conclude that people close to the attacker noticed something or knew that something was not right. There are indicators we can identify along with providing ways and means to be alerted to potential danger. Continuing this strong focus is important and exceeds the purview of TSA and DHS into the entire federal government. Mr. Pekoske anticipates engaging in a dialogue about this topic when he returns to TSA.

Regarding cyber threats and ransomware attacks, Secretary Mayorkas focused on ransomware when he came into office in February, 2021. Significant attention and great interest is now concentrated on the nefarious use of cryptocurrency as a way to make money that can not only be used to influence populations but also to create anxiety with the potential for significant damage. The recently stood-up Cybersecurity and Infrastructure Security Agency's (CISA) primary role is the prevention of cyberattacks and ransomware attacks. The agency's responsibilities include developing a response posture for attacks. Intentions are to focus efforts to improve upon prevention and response. CISA plans to complete a series of sprints with focus on a particular topic for 60 days. The current topic is ransomware. Transportation security will be the topic in the fall.

Because surface transportation critical infrastructure is largely held by private entities, Mr. Pekoske emphasized the importance of sharing information with owner/operators offering the opportunity for it to be enhanced significantly by the private sector's expertise. To that end, government intelligence offices are trying to find more efficient ways to access and share information with stakeholders. Attention should also be directed to new processes for security clearances that would reduce periodic investigations and verify that the clearance holder continues to meet requirements. An enhanced approach to the periodic five-year checks might aim at obtaining alerts from continual checking by making the portability of clearances much easier. For example, if an individual is working for a rail company and then moves to a pipeline or a trucking company, the clearance would transfer over.

Mr. Pekoske is looking forward to getting over COVID-19 precautions and would like to see a return to the workplace. He anticipated meetings in the not too distant future taking place in person, as it is a good way to exchange information.

Mr. Pekoske thanked Ms. Victoria Newhouse and Ms. Judith Harroun-Lord for their TSA leadership roles with the Committee and additionally thanked the STSAC leadership and Committee members for their participation.

Ms. Newhouse thanked Mr. Pekoske for his remarks and the STSAC Chair and Vice Chair for the countless hours they have dedicated to working behind the scenes with the Committee in order to complete major milestones. She acknowledged the Aviation Security Advisory Committee (ASAC) Chair and Vice Chair, noting the two advisory committees are closely aligned and that the STSAC and ASAC continually learn from each other.

## Chair and Vice Chair Opening Remarks

Chair Farmer echoed sentiments previously expressed about commitment and the countless hours and thorough and effective efforts devoted by all members, industry and government, often on weekends or at night. All of this added work came during a time of unprecedented challenges including a pandemic, demonstrations resulting in acts of violence, cyberattacks, a rise in domestic extremism, and weather events. Everyone has had to manage the effects of these developments within their own organizations and then, in addition, meet their responsibilities in the STSAC and its subcommittees.

Mr. Farmer also shared a short baseball analogy with the Committee, based on the book and film, “Moneyball.” The Oakland Athletics baseball team has consistently produced exceptional talent – but lacked the resources to afford retaining these players as they became eligible for free agency and bidding by other teams for their services. After the 2001 season, in which the A’s again made the playoffs, multiple All-Star caliber players departed. For 2002, the team had to be reassembled. In this effort, the team focused on a basic theme: “What do we like about him? He gets on base.” How did not matter – hit, walk, error, other means. Baserunners are a disruptive force, causing distractions and escalating pressure on pitchers, catchers, and the other fielders. With lower cost players who excelled at getting on base, Oakland defied the experts, won 102 games – more than the previous season, and again made the playoffs.

When reviewing the recommendations, Mr. Farmer considered them in the context of key threats—highlighting the intent to provide a means to get surface transportation on base and, subsequently, narrow the opportunity for adversaries to cause harm. The 18 unanimously approved recommendations present three themes: (1) enhance profile, (2) expand access to existing structures, and (3) effective use of threat and security information. Gaining and maintaining increased access to and expanded use of threat intelligence and related security information are vital to addressing new threats effectively. Analyses of terrorist and violent extremists attacks, failed attempts, and disrupted plots consistently show – there are always indicators of the developing threat. It is frequently not a matter of whether indicators are present, but rather if their significance is recognized. Highlighting these indicators affords opportunities for training workers and police and for informing the public on what to look out for and how to report those observations effectively. Similarly, focus on indicators of concern and compromise can inform sustained implementation of effective cyber risk mitigation measures. CISA and the FBI continue to do very well in addressing the risks associated with specific cyber attack campaigns and means to mitigate exposure to breaches and exploitations. However, we still need to learn and apply lessons for enhanced cybersecurity based on the indicators gleaned from analyses of and reporting on cyber threats, incidents, and security concerns. The fundamental premise of key recommendations of each of the subcommittee is surface transportation organizations reporting on suspect, anomalous, or otherwise odd activity, physical and cyber, and sharing that reporting, properly anonymized, with government and colleagues across modes of transportation. This type of timely reporting can highlight developing threats or significant security concerns and create opportunities for prevention.

Mr. Farmer expressed how the subcommittees have aligned their efforts with the priorities in the Administrator's tasking letter. Industry and government developed the priorities together, which ultimately led to the development of the recommendations to fulfill those priorities. He also stated that the Committee should be proud of these interactions as they are making a difference.

Mr. Farmer discussed what can be done collectively by getting surface on base. "What can I do to limit adversaries?" "What can I do to raise my posture?" Visual deterrents are key. It is important that transportation organizations share what they are seeing and government can look across all modes and networks to determine if there is a system-wide threat.

Ms. Hanson thanked Mr. Pekoske and highlighted how the group has worked exceptionally hard since April 2020 when their first virtual meeting was held. She highlighted how the Committee has addressed the COVID-19 threat, addressed employee concerns, and made surface transportation workers a priority. Ms. Hanson also thanked everyone for their commitment and accomplishments since that meeting, including the 18 unanimously approved recommendations that the Committee just heard were accepted by Mr. Pekoske. The Committee may have felt like nobody noticed, but a lot has been going on. This included the face mask SD, significant cyberattacks, and new threats from domestic violent extremists.

Ms. Hanson stated that the subcommittees will highlight what they can implement now and what else they can achieve by developing a roadmap that will include steps that need to be taken to reach milestones they want to accomplish by the very ambitious goal of July, 2022. The subcommittee members and their contributions are making surface transportation even stronger, and surface transportation will thrive because of their service.

## Cybersecurity Threat Brief

Mr. Anthony Lewis, TSA Intelligence and Analysis (I&A), provided an update on threats to surface transportation in the homeland. His brief included physical threats to freight rail, mass transit, passenger rail, highway motor carrier, and hazardous liquid and natural gas pipelines. He also provided an overview on the recent national terrorism advisory system bulletin that the DHS issued regarding the heightened threat environment in the United States. He advised his listeners that his brief contained unclassified sensitive security information and to handle it accordingly. Consistent with applicable state, local, tribal, and territorial laws, law enforcement organizations should maintain situational awareness of online and physical activities that may be related to an evolving threat of violence. The NTAS is set to expire on August 13, 2021. In conclusion, Mr. Lewis thanked everyone for their time.

## Ransomware and DVE Brief

Mr. Christopher Wheat, Federal Bureau of Investigation (FBI) cyber division analyst, provided an update of the current ransomware threat landscape, some of which was sensitive information.

Mr. Wheat explained that ransomware is a form of malware that encrypts a user's files, and makes them inaccessible and unusable until a ransom is paid. Ransomware, as a concept, has actually existed since the late 1990s. Mr. Wheat believed there was a security researcher who had a form of proof of concept that was distributed via floppy disk. However, building onto what Acting Deputy Secretary Pekoske stated earlier, ransomware as a criminal scheme really wasn't profitable until the advent of cryptocurrency around the 2013 timeframe, making the cash out aspect of the criminal scheme more anonymous. Since 2013, ransomware has become a viable criminal scheme and its development should be reviewed in two phases.

First, during the period of 2013 to late 2017 or early 2018 when the primary set for ransomware was broad, indiscriminant, and not very sophisticated, attacks cast a very wide net trying to encrypt both large targets and smaller alike. The best example of that was the WannaCry Ransomware Campaign, an obviously very disruptive ransomware campaign, but not all that profitable.

Second, in late 2017 into 2018, ransomware actors were becoming progressively more sophisticated and skilled, and their malware much more advanced. That is when the FBI began to see some of the more disruptive, and ultimately profitable attacks, particularly against critical infrastructure sectors.

Essentially a trend has continued from early 2018 to the present, where over time, there has been a steady increase in ransom demands to the point we are seeing demands in the tens of millions of dollars. Whereas, if you went back to the early days of ransomware in 2013, you would typically see ransoms in the range of $300.00 to $700.00. Another important trend that we have seen since late 2019 is the rise of data exfiltration as a component of ransomware campaigns. The Maze ransomware variant was the first to do that consistently in the United States. However, there are still a few ransomware variants that do not exfiltrate victim data before encrypting the victim’s system.

Mr. Wheat noted the private sector is the main target at risk, and the government needs the capability to defend. The agency’s working relationship with the private sector is critical to the development and application of an effective response to ransomware. The agency worked extensively over the past few years to build relationships with the private sector, ingesting as much data as possible from the private sector, and developing and improving two-way information sharing to assist with pushing out indicators of compromise as soon as they are visible.

Mr. Wheat thanked everyone for their time and turned the meeting over to his colleague, Mr. Walter Gilmour, to discuss domestic terrorism threats.

Mr. Gilmore provided a brief domestic terrorism threat overview.According to U.S. Code, the legal definition for domestic terrorism is defined as any act dangerous to human life that violates United States criminal laws and appears to be intended to intimidate or coerce the civilian population, influence the policy of a government or affect the conduct of a government by mass destruction, assassination, or kidnapping. It is important to note that there is no specific domestic terrorism charge. However, the FBI and DHS define those who participate in domestic acts that would be considered domestic terrorism as a Domestic Violent Extremist (DVE)—an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts or force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute extremism, and may be constitutionally protected. While it is important to be aware of these different ideologies, violence is the most important focus.

Mr. Gilmour discussed five threat categories—(1) racially or ethnically motivated violent extremism (RMVE) that uses political and religious justification to support racially or ethnically motivated ideologies; (2) anti-government, anti-authority, and violent extremism encompassing the unlawful use or threat of force of violence in furtherance of agendas, derived from anti-government, anti-authority sentiments, which include opposition to perceived economics, and social hierarchies, perceived government overreach, negligence and even illegitimacy. Subsets included focus on targets or symbols of capitalism, law enforcement, and government, militia which targets perception of law enforcement overreach in regard to certain areas such as gun control or land rights, and sovereign citizen violent extremism; (3) animal rights and environmental violent extremism; (4) abortion-related violent extremism that includes threats of violence based on ideological agendas either for or against abortion from both the pro-life and the pro-choice side; and (5) all other domestic terrorism threats encompassing individuals who use force, violence, or threats of force of violence in the furtherance of political ideology, who are more idiosyncratic and do not fall neatly into one of the other four categories.

The FBI assessed that the greatest threat to the homeland is still lone actors who are self-radicalized online with no formal connection to a group, looking to attack soft targets with easily accessible weapons. The agency continues to work with other government agencies as well as with state and local partners to mitigate the continued threat of individuals who are unknown to law enforcement combined with the opportunistic and event-driven nature of this type of extremist violence.

## DarkSide Ransomware

Mr. Christopher Phair, a Cyber Intelligence Analyst with the DHS Office of Intelligence and Analysis, Cyber Mission Center (CYMC), provided a mostly open source brief on the DarkSide ransomware actors who attacked a major United States fuel system and forced the company to halt operations. The company reportedly paid the attackers nearly $5 Million in ransom shortly after the attack in order to recover access to their network. This case highlighted the difficulty faced by critical infrastructure victims who decide to pay ransoms to maintain continuity of critical operations.

DarkSide has been observed in ransomware campaigns since at least August of 2020; victim organizations have been primarily based in the United States and span across multiple sectors including energy and critical manufacturing. DarkSide actors have largely relied on open-source and commercially available IT tools to facilitate stages of their attacks, as these tools are widely used and obscure attribution to particular actors if they are found on a victim network.

Notably, DarkSide appears to have a partnership with a Trojan botnet malware known as ZLoader or Silent Night. This partnership highlights an important development in ransomware attacks over the few years, as ransomware-as-a-service operators often rely on initial access to victims from other organized criminal groups who operate Trojan botnets such as Emotet and Trickbot, which have been in the news recently.

According to public reporting, about $90 million in Bitcoin ransom payments from 47 distinct wallets were made to DarkSide and 99 organizations have been infected with the DarkSide malware, suggesting that approximately 47% of victims paid a ransom, and that the average payment was $1.9 million.

A DarkSide actor stated that affiliates are prohibited from targeting hospitals, schools, universities, non-profit organizations, and public sector entities. Following the major United States fuel system attack, DarkSide claimed their goal was to make money and not create problems for society.

CISA and FBI recently issued a Joint Advisory on DarkSide ransomware in which they urge CI asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in the mitigations section including implementing robust network segmentation between IT and OT networks; regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections. These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.

## Subcommittee Update and Implementation Plans

Mr. Farmer encouraged participants, particularly industry, to reach out should questions arise after the meeting. Questions can be brought to Ms. Hanson, Mr. Farmer, or the TSA STSAC Mailbox. Mr. Farmer noted the primary goal of this meeting is extracting insights that can be beneficial to what this Committee can accomplish to support or complement efforts and capabilities of surface transportation organizations for security and emergency preparedness.

Mr. Farmer and Ms. Hanson introduced the foresight to the Committee's focused attention for today's discussion. Looking ahead, the Committee reached a major milestone in the submission of 18 recommendations to the TSA Administrator. Today, the Committee received validation from Acting Deputy Secretary of Homeland Security Pekoske that all 18 recommendations were accepted. The Committee appreciated that effort and the Administrator's support. Mr. Farmer expressed particular appreciation for the participation in today's meeting of executives across the various functional areas of TSA showing commitment to this collective effort.

Mr. Farmer proposed two questions to the Committee. First, "What recommendations are amenable to implementation now or in the very near term?" Second, "What can we accomplish in that implementation through the work of the expertise assembled in this Committee, both industry and government, supported by key leads at TSA, and its partners?" Mr. Farmer announced that today's subcommittee presentations will focus on the recommendations that are amenable to implementation now.

The Committee will focus on providing additional effort over a longer period of time for the recommendations requiring long-term implementation. Based on what Ms. Hanson cited earlier, the Committee is committed to having a roadmap that will include steps that need to be taken to reach near-term milestones they want to accomplish by July 2022.

The roadmap, a term that SOPD TSA Administrator Darby LaJoye used during a discussion earlier this week with Mr. Farmer and Ms. Hanson, will outline implementation plans of the recommendations. Mr. Farmer stated that it will highlight recommendations that can be done immediately or in the very near term, and those that will take a little bit more time and effort.

Overall, the goal is to assemble the necessary steps that need to be taken and then align the work to put those steps into action.

Ms. Hanson thanked the subcommittee co-chairs, both industry and government and looked forward to hearing the presentations today.

**Security Risk and Intelligence Subcommittee**

Jim Cook, the Assistant Chief of Police for the Amtrak police department, introduced the work completed in progress to date by the Security Risk and Intelligence Subcommittee. There has been a substantial amount of progress done since the last STSAC meeting in February, 2021. For subcommittee specifics, Mr. Cook turned the meeting over to Darnell Young for continued discussion.

Darnell Young, TSA I&A and the Designated Federal Officer for the Security Risk and Intelligence Subcommittee, provided a briefing on the four recommendations submitted by the Security Risk and Intelligence Subcommittee and the actions the subcommittee is taking in the short term and long term to implement all four recommendations. During the preceding quarter, the Security Risk and Intelligence Subcommittee initiative has been meeting regularly at the working group level. As a team, the subcommittee reached out and hosted discussions with partners at TSA, DHS, and the Office of the Director of National Intelligence (ODNI).

Mr. Young referenced the following four recommendations:

> **STSAC Security Risk and Intelligence FY2021 Recommendation #1:** Establish a National Intelligence Manager for surface transportation through an official request by the TSA Administrator to his/her equivalent at the Office of the Director of National Intelligence (ODNI) for designation and sustainment of this position to ensure effective and sustained leadership and management and to support increased surface intelligence threat reporting and information sharing across the Intelligence Community with surface transportation stakeholders.
>
> **STSAC Security Risk and Intelligence FY2021 Recommendation #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, including the DHS Homeland Security Intelligence Priorities Framework (HSIPF), through consolidation of current requirements, updated annually, in a joint effort of the STSAC's Security Risk and Intelligence Subcommittee and TSA's Surface Information Sharing Cell that assures continuous awareness and understanding of surface transportation priorities and needs.
>
> **STSAC Security Risk and Intelligence FY2021 Recommendation #3:** Approve and implement the Surface Information Sharing Cell (SISC) charter by attaining the TSA Administrator's written concurrence with the provisions and procedures for assuring clarity and consistency in governance, membership, roles, responsibilities, and protection of classified threat intelligence and security information and timely and effective two-way surface transportation threat intelligence/information sharing across government and the private sector.
>
> **STSAC Security Risk and Intelligence FY2021 Recommendation #4**: Complete the Security Risk Methodology Matrix as a resource to support efforts to drive down risk across

surface transportation modes by developing and maintaining, through recurring reviews and updates, the Security Risk Methodology Catalog to provide a detailed overview of widely used risk assessment and mitigation models and tools employed by surface transportation stakeholders and to inform and enhance efforts to identify, analyze, and measure risk and set security priorities for prevention and response capabilities.

Mr. Young began his briefing with recommendation three based on its short-term implementation. The establishment of the Executive Steering Committee requires key senior leaders from both industry and government to drive success and move forward with approval. Specifically, TSA will send letters to industry organizations, and federal government agencies, requesting assignment of a senior leader to serve on the SISC Executive Steering Committee.

The goal is to have an industry Executive Steering Committee and a government Executive Steering Committee established. The subcommittee recommended industry and government leaders meet to discuss internal issues at the executive level prior to drafting the charter and joint governance. The charter and joint governance will be developed collaboratively with the assistance and input of subject matter experts from industry and government. Mr. Young stated that the subcommittee should see full operational capability in the next 9 to 12 months. The SISC will gather feedback on the progress of the program on an annual basis.

Mr. Young proceeded to discuss the first recommendation—the establishment of a surface National Intelligence Manager (NIM).

The prominent near-term initiatives for this recommendation are to continue discussions with TSA, DHS, and ODNI on the best organization for the surface transportation NIM. During the coming months, the subcommittee plans to consolidate expectations from industry as well as government, for a national intelligence strategy to include ODNI, and, potentially, the Department of Defense (DoD).

Thereafter, TSA plans to submit a white paper to DHS and ODNI with the industry request and supporting rationale for the surface transportation NIM at the ODNI level. This paper will cover the near- and longer-term benefits that will result. The request may entail restructuring of billets, and/or request for additional funding, however, the goal is to regularly hold discussions through the SISC Executive Council on major issues to move forward the efforts on the surface transportation NIM. Understanding these challenges, this recommendation may take longer because of the potential restructuring.

Mr. Young proceeded to discuss the second recommendation.

The working group tasked to this recommendation has done a lot of work for the subcommittee as actions have already been taken to move forward towards implementation. TSA will review, validate, synchronize, and cross-check requirements against existing requirements. The next step in implementation requires TSA to make a united effort across the government to consolidate industry requirements to inform the intelligence community. Regarding the longer-term efforts, an annual or biannual update will be completed which will include additional industry requirements.

Mr. Young discussed the fourth recommendation—the completion of a security risk methodology matrix spanning across all surface transportation modes. The Requirements Capability and Analysis (RCA) office will work with industry subject matter experts to create a concise but comprehensive overview of how each model identifies, analyzes, and measures risk.

Once feedback is received, the RCA office will compile collected details into one catalog, which will be distributed back to the STSAC Committee for final review and feedback before final submission to the TSA Administrator. No significant long-term efforts were identified, however, the periodic review and/or updates of the catalog would be part of sustained long-term efforts.

### Cybersecurity Information Sharing Subcommittee

Mr. Lee Allen, Designated Federal Officer for the Cybersecurity Information Sharing Subcommittee, provided a brief introduction and reviewed the subcommittee's four recommendations and their short-term and long-term implementation plans.

Mr. Allen referenced the following four recommendations:

> **STSAC Cybersecurity FY2021 Recommendation #1:** Establish a surface transportation cyber information sharing network on threats, incidents, and security concerns and related alerts, advisories, analyses, and assessments by having the Surface Information Sharing Cell (SISC) serve as the hub, with spokes assuring engagement with organizations in each surface transportation mode, for the exchange of reporting, analyses, advisories, and alerts on cyber threats, incidents, and security concerns – with necessary analytical support.
>
> **STSAC Cybersecurity FY2021 Recommendation #2**: Manage the operations of the Surface Information Sharing Cell (SISC) under the express authorization provided by the Cybersecurity Information Sharing Act of 2015 by convening meetings with interagency partners, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS/CISA) and the Department of Justice, to ensure the authorizations and protections accorded by the Cybersecurity Information Sharing Act of 2015 are applied in managing the operations of the SISC.
>
> **STSAC Cybersecurity FY2021 Recommendation #3**: Establish effective procedures for broad sharing of cyber threat and security information across surface transportation modes, with industry governance, by leveraging proven means already in place through industry initiatives.
>
> **STSAC Cybersecurity FY2021 Recommendation #4**: Conduct an annual review to assess the performance and impact of the Surface Information Sharing Cell (SISC) in its core functions of threat information distribution, analytics, relevance, and actionable intelligence– through a joint team comprised of government officials and industry representatives.

Mr. Allen highlighted recommendation number one—the establishment of the surface transportation cybersecurity information sharing network for threats, incidents, security concerns, and related alerts, advisories, analyses, and measures.

Mr. Allen addressed recommendation number two—to manage the operations of the Surface Information Sharing Cell (SISC) based on the express authorization provided by the Cybersecurity Information Sharing Act of 2015. He noted several federal publications that offer guidance on sharing cybersecurity information. One of the tools the subcommittee is researching is a product called Special Publication 800-150, which is a guide to cyber threat information sharing. It complements the Cyber Security Sharing Act of 2015. An additional avenue the subcommittee is exploring includes the standards that have been developed by DHS for Information sharing organizations (ISOs). The subcommittee intends to review the CISA program for recommendation implementation planning. TSA must agree with identifying federal partners for coordinated effort to ensure statutory provisions of, and associated guidance for, the Cybersecurity Information Sharing Act of 2015 are applied, as appropriate, to guide the work of the SISC.

Mr. Allen discussed recommendation number three—establishing effective procedures for broad sharing of cyber threat and security information across surface transportation modes. This recommendation coincides with the work that the Security Risk and Intelligence Subcommittee is doing as well.

He followed with the fourth recommendation—conducting an annual review to assess the performance and impact of the SISC. This recommendation could require longer term efforts. He outlined the actions needed to coordinate with multiple federal agencies and other resources.

Mr. Allen explained how the subcommittee intends to focus on recommendations one, three, and four for short-term implementation – to include ensuring that the SISC has the required documentation in place to allow the participation of relevant key stakeholders. Priority information sharing procedures will need to be established – with identified capabilities and processes to make implementation possible. Additionally, recurring communication links with stakeholders will need to take place – including working continuous coordination with the Security Risk and Intelligence Subcommittee. The goal is to assess and adopt recommended communication platforms for broad and efficient communication with stakeholders.

Mr. Farmer added additional comments to Mr. Allen's briefing, addressing three of the recommendations attainable for the near term, how that may be accomplished, and the benefit their accomplishment will bring to cybersecurity posture in surface transportation. The emphasis on the Cybersecurity Information Sharing Act of 2015 derives from what the statute specifically authorizes in terms of information sharing – within industries, across sectors, and between government and industry, and vice-versa. This act has two significant elements that are especially beneficial in addressing long -standing private sector concerns – affording protections against antitrust liability and civil liability for uses of sharing cyber threat and security information for the intended purposes. The potential for some form of liability is often a principal concern for private sector organizations in terms of how information is shared. An Executive Order was issued near the end of the last presidential administration that focused on looking at the Cybersecurity Information Sharing Act of 2015 and its implementation. The work of this subcommittee aligns with the objective of that executive order.

## <u>Insider Threat Subcommittee</u>

Colonel Michael Licata, an industry Co-Chair of the Insider Threat Subcommittee, provided opening remarks for the subcommittee. Mr. Licata thanked government Co-Chair Matthew Hudren and Designated Federal Officer Dean Walter for walking the subcommittee through this process and sharing their wisdom. Both Mr. Hudren and Mr. Walter provided the subcommittee with productive leads that will make implementation easier.

Mr. Hudren began discussion for the subcommittee and mentioned that the subcommittee is currently waiting for TSA to make the next move, considering a lot of the subcommittee's recommendations require the resources and authority of TSA.

Mr. Hudren referenced the following eight recommendations:

> **STSAC Insider Threat FY2021 Recommendation #1:** 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 to raise awareness and share effective practices on threat detection, risk assessment, intelligence priorities, and response techniques.

**STSAC Insider Threat FY2021 Recommendation #2:** Develop a Case Optimization and Risk Evaluation (CORE) tool by applying analyses of, and lessons learned from, case studies of insider incidents that have affected transportation organizations, and related research and development efforts, to identify and communicate key threat indicators, facilitate production of educational materials, guide training and awareness initiatives, and inform implementation of sustainable risk mitigating measures.

**STSAC Insider Threat FY2021 Recommendation #3:** Implement a nationwide online tip capability that provides a timely and simple means to report suspicious activity and threats for transportation industries, entities, or individual operators lacking well-defined organizational structures and procedures for reporting significant security concerns.

**STSAC Insider Threat FY2021 Recommendation #4:** Define parameters for assessing the level of potential insider threat risk posed to organizations in the surface transportation modes–high, medium, or low–based on categories, functions, or level of access of employees, contractors, and vendors.

**STSAC Insider Threat FY2021 Recommendation #5:** Produce and disseminate recommendations on effective practices for workforce vetting programs for surface transportation organizations tailored to the high, medium, and low risk categories and guided by the matrices developed by STSAC's Insider Threat Subcommittee.

**STSAC Insider Threat FY2021 Recommendation #6:** Expand the scope of participation in TSA's existing Insider Threat Executive Steering Committee by including representatives of the STSAC and ASAC to coordinate insider threat analysis and risk mitigation efforts for the aviation, surface, and maritime transportation industries.

**STSAC Insider Threat FY2021 Recommendation #7:** Establish a consistent coordination process to facilitate communication of sensitive information on reports or allegations of terrorist or extremist ties, or suspected illicit insider activity, on transportation workers by federal law enforcement, security, and intelligence agencies with the employing or contracting transportation organization.

**STSAC Insider Threat FY2021 Recommendation #8:** Maintain a consolidated insider threat information resource for transportation on the Homeland Security Information Network (HSIN) to facilitate access to and usage of assessments, advisories, and analyses up to the sensitive security information (SSI) level.

Mr. Hudren stated that recommendations one through three are already in place and suggested they should be very simple to implement. The second recommendation—developing a case optimization risk evaluation tool—is already a part of the ASAC recommendations. Mr. Hudren expressed that this subcommittee would like to be a part of the ASAC's insider threat efforts, working jointly.

Mr. Scott Gorton, Executive Director, Surface Policy Division, PPE, provided feedback to Mr. Hudren that while TSA has considered these recommendations and concurred with all eight, while certain conditions remain that TSA will have to work through including working with the members of the subcommittee and the overall STSAC to iron out details and complexities. This is because items like the Integrated Risk Management Mitigation tool already exist. Mr. Gorton suggested leveraging existing programs that have been initiated as well as those in various states of development that would benefit obtaining a maximum advantage for surface transportation. Budget and resource plans will have to be made to implement these recommendations.

Mr. Gorton expressed how TSA can work with the Committee members to outline requirements, vision statements, and issues that need to be addressed so a path forward can be developed. Regarding one of the subcommittee's recommendations to establish an information sharing portal, the ASAC and TSA have been working to have this portal established. Associated discussions have taken place to set up the portal, publicize it, and provide access to stakeholders. This recommendation is nearing completion.

Mr. Gorton echoed his appreciation for the TSA executive leadership members who were attending the meeting expressly to hear the recommendations. Implementation of these recommendations is an enterprise wide effort that spans across multiple offices within TSA and the STSAC will need their support. TSA's Law Enforcement and Federal Air Marshal Service is taking the lead on enrollment services and vetting programs as this office certainly has expertise to offer.

Mr. Gorton expressed how some recommendations are more complex and may have legal issues that have to be resolved and resourcing challenges to overcome.

Mr. Hudren discussed the recommendations for short-term implementation, including a nationwide tip line within the TSA Transportation Security Operations Center (TSOC) which already has an operational cell established for suspicious activity reporting that might be leveraged.

Mr. Hudren proceeded to review recommendations four, five, and seven. Recommendation four—parameters for assessing the level of potential insider threat risk posed to organizations within surface transportation modes—will take some work. Recommendation five—producing and disseminating recommendations and accepted practices for workforce vetting programs—what about it (did he say anything in particular)? Recommendation seven—establishes consistent processes and facilitates communication by federal agencies to surface transportation organizations—will take some time to implement as case studies need to be analyzed for indicators. Mr. Hudren suggested that the work to analyze case studies be outsourced via contract.

Mr. Hudren thanked Mr. Gorton for providing insight based on the problems the subcommittee has faced. Mr. Hudren expressed his goal to uncover unforeseen threats that cannot be seen now by bringing together the surface transportation modes alongside the ASAC members. TSA's help and support is much appreciated in accomplishing that.

Mr. Gorton agreed with Mr. Hudren, echoing the large undertaking that includes the entire workforce in surface transportation. Mr. Gorton suggested approaching this hurdle in logical steps in order to prioritize and develop tools to look at insider threat risk for surface transportation, properly characterize it, and establish the most appropriate programs to address the risk. Mr. Gorton emphasized it will take a lot of effort and collaboration from multiple offices and stakeholders to achieve these goals.

## Emergency Management and Resiliency Subcommittee

Mr. Christopher McKay, the government Co-Chair for the Emergency Management and Resiliency Subcommittee, provided a brief introduction. Mr. McKay thanked everyone for the opportunity to brief out the activities of this subcommittee and stated that he wanted to discuss a proposed path forward.

This subcommittee agreed early on, in light of the pandemic, to work on developing and sharing best practices and recommendations in regard to COVID-19. As a result, the subcommittee conducted a workshop in September 2020. After the workshop, an after-action report was prepared on best practices and lessons learned that was widely distributed to industry and government. Subsequently, the subcommittee developed two recommendations which are assessed as achievable in the short and medium term.

Mr. McKay referenced the following two recommendations:

> **STSAC Emergency Management and Resiliency FY2021 Recommendation #1**: Enhance pandemic preparedness by sharing lessons learned on response to COVID-19 across modes by working with government and industry partners to disseminate the Emergency Management and Resilience Subcommittee's report on pandemic response in surface transportation, produced from the COVID-19 Best Practices and Lessons Learned Workshop, to include posting on respective government websites and, where applicable, incorporating into security and emergency preparedness resources maintained by TSA and DOT.
>
> **STSAC Emergency Management and Resiliency FY2021 Recommendation #2:** Support COVID continuing education to enhance response capabilities and resiliency by TSA and industry partners working jointly through the Subcommittee to maintain a process for the recurring review and update of the report on effective practices and lessons learned and supporting information, as warranted, based on input received or obtained on the continuing effects of the COVID-19 pandemic; disruptions caused by surges of confirmed cases nationally; and responses by surface transportation organizations – with particular emphasis on indications of improved performance based on application of lessons learned.

Mr. McKay turned the meeting over to the subcommittee's industry Co-Chair Jennifer Gibson for the implementation planning review on its two recommendations.

Ms. Gibson highlighted that the subcommittee is focused on publishing relevant materials regarding best practices and lessons learned on relevant websites such as TSA.gov and transportation.gov (DOT). All reports will be made widely available and will be distributed to several groups and sector councils. The second element of importance was that all reports and material remain updated on those sites. Ms. Gibson suggested these items as short-term, immediate items for implementation.

Ms. Gibson further explained that recommendation number two was viewed more as an ongoing report since information has changed from the time when the workshop was held in 2020. The subcommittee was planning to reconvene to discuss the progress that made since the 2020 workshop and determine next steps. Issues such as vaccine distribution have been presented since the document was first released. The subcommittee may consider another workshop to revisit these topics as an ongoing effort. Ms. Gibson stated the subcommittee will meet again in mid-June to determine a path forward.

Mr. Farmer thanked Ms. Gibson for the update and broader perspective on applying lessons learned, particularly with vaccine distribution. Mr. Farmer believed this subcommittee gave the Committee a chance to look at how surface transportation is affected by and responds to various contingencies. Mr. Farmer thanked all members of the Emergency Management and Resiliency Subcommittee for their efforts.

## Vote to Accept February 18, 2021 Meeting Minutes

Mr. Farmer instructed members of the Committee of the need to take action on the meeting held February 18, 2021. Minutes for this meeting had been distributed in advance to Committee members for their review. Mr. Farmer requested a motion to accept the February 18, 2021, minutes. A motion was moved to accept the minutes and the motion was seconded. The motion carried by voice vote and the minutes were accepted.

## Committee Administrative Discussion

Scott Gorton briefly discussed the extension of the training rule from March 22 to June 21, 2021. This extension should provide sufficient time to submit security training programs. The American Public Transportation Association (APTA) hosted a webinar in May for agencies to submit tips and lessons learned. TSA has learned lessons about transmitting large files and is currently working out technological bugs. A total of 51 training programs have been submitted, with two approved. Particularly, one member of this Committee was one of the first ones to get their submission approved. There were 15 submissions still in the process to receive approval letters. TSA was working to get everything approved—so far companies have been receptive to that.

Mr. Gorton discussed the current mask mandates. There was a lot of government communication between DOT, TSA/DHS, USCG, and the CDC recognizing there were several questions regarding state requirements. TSA was researching the possibility of relief for workers in outdoor situations. TSA hosted listening sessions with carriers to obtain feedback and provide greater clarity for guidance. Mr. Gorton highlighted that requirement for passengers in conveyances will remain the same. TSA will appropriately message all guidance so that employees and employers are aware of what to do.

## Senior Official Performing Duties (SOPD) of the Administrator Closing Remarks

Senior Official Performing the Duties (SOPD) of the Administrator Darby LaJoye provided closing remarks.

Mr. LaJoye voiced appreciation for everyone's efforts which were extremely valuable to the entire country. Mr. LaJoye had the pleasure of conversing with the STSAC Chair and Vice Chair during a previously held meeting. Mr. LaJoye agreed that the sustained areas of focus and the key to enhancing security is to maintain a close collaborative partnership. Mr. LaJoye was fully committed to understanding industry's needs.

Regarding recent events in the pipeline sector, the highest levels of government recognized this as a national security issue. TSA was and is actively engaged with industry partners, CISA, and Congress on what efforts can be achieved in the immediate and longer-term future to reduce exposure. Mr. LaJoye stated there has been a lot of focus on this topic for a while. A total of 23 Pipeline Cybersecurity Initiatives have been completed with 29 more scheduled for near-term.

Mr. LaJoye anticipated completing all 52 initiatives by the end of 2021. These initiatives provide stakeholders with a picture of strength, vulnerabilities, and key trends across the industry.

Mr. LaJoye stressed the need for and importance of efficient, effective information sharing across all surface transportation modes so that industry has the essential information required to make key decisions. This topic, in particular, was discussed with the STSAC Chair and Vice Chair.

Mr. LaJoye thanked the Committee for the STSAC 2020 Annual Report, a testament to the time and commitment dedicated to this mission. Mr. LaJoye concurred with all 18 recommendations and stated that Mr. Scott Gorton and Ms. Sonya Proctor were working with other offices to obtain responses in the next 30 days. TSA will obtain the resources needed to make collaborative efforts successful. Agreeing is easy—it will take a lot of work to achieve solutions.

Mr. LaJoye thanked everyone again and stated that he could not ask for better partners. He hoped to meet the Committee members in person in the near future.

Mr. Gorton mentioned that the new TSA headquarters has a Memorial Hall with a timeline of significant events in TSA's history. Included on that timeline is the STSAC creation etched in glass. Mr. Gorton expressed he would love the Committee to see this memorialization in person in the near future.

Mr. Farmer expressed additional appreciation for the support and looked forward to progressing on the recommendations.

## STSAC Executive Sponsor Closing Remarks

STSAC Executive Sponsor Victoria Newhouse (PPE Deputy Assistant Administrator) provided closing remarks.

Ms. Newhouse thanked Mr. LaJoye for his remarks. Ms. Newhouse highlighted that Mr. Pekoske at the beginning and Mr. LaJoye at the end demonstrated TSA top leadership's commitment to the STSAC. Ms. Newhouse thanked the STSAC Chair and Vice Chair for their remarks and the ground they covered today. She appreciated the commitment from top leaders in TSA and the ASAC who will assist the STSAC Insider Threat Subcommittee. TSA will continue the momentum and sharing of information. Ms. Newhouse anticipated more to be achieved over the summer with meetings to review the implementation planning progress. Ms. Newhouse echoed the invitation to come to TSA Headquarters to see the Memorial Hall.

DFO Harroun-Lord thanked to everyone who provided remarks and for their commitment to the STSAC.

## Adjournment

DFO Harroun-Lord sought a motion to adjourn the meeting. Michael Beltranena, Jr. motioned to adjourn the meeting. Natalie Jones-Best seconded the motion. The motion to adjourn was carried by a voice vote of the Committee.

The eighth meeting of the STSAC meeting was adjourned at 3:57 p.m. EST.

**Certification of STSAC May 20 Meeting Minutes**

*I hereby certify that is an accurate record of the activities of the Surface Transportation Security Advisory Committee on May 20, 2021.*

Thomas L. Farmer

Thomas L. Farmer
Surface Transportation Security Advisory Committee Chair