Surface Transportation Security Advisory Committee

Annual Report to the Administrator of the Transportation Security Administration (TSA) and Congress of the United States for 2021 - 2022

December 2022

In accordance with the requirements of the *TSA Modernization Act of 2018*, the Surface Transportation Security Advisory Committee (STSAC) submits this annual report on its priorities, activities, and accomplishments to the TSA Administrator and to multiple committees of the United States Congress. The period covered extends beyond a year – from the submission of the inaugural annual report in April 2021 through December 2022 – based on the express determination of the Committee's elected officers. The level of progress attained in the four subcommittees' efforts to complete implementation of the unanimously approved recommendations to the TSA Administrator merited affording added time for completion – and documentation in the STSAC's second annual report. Additionally, during the latter part of this period, the Administrator initiated the succession process for voting membership in the Committee. With the extension, the report captures in full the exceptionally dedicated efforts, and the progress attained as a result, of the appointees to the Committee whose service commenced with the opening session held in July 2019 – as well as those added with the expansion in voting membership effected by appointments of new members, with emphasis on cybersecurity expertise, who convened for the first time at the November 2021 public meeting.

This report addresses the following subjects:

1) Purpose of the STSAC
2) Meetings of the STSAC and Subcommittees
3) Implementation of the Approved Recommendations to the TSA Administrator
4) Acknowledgments
5) Appendices:
    a. Appendix A: STSAC – Timeline of Activities
    b. Appendix B: Approved Recommendations of the STSAC to the TSA Administrator (February 2, 2021)

1) **Purpose of the STSAC**:

In accordance with its legislative mandate, the STSAC serves as the principal forum to "advise, consult with, report to, and make recommendations to the Administrator on surface transportation security matters." (Homeland Security Act of 2002, as amended – Section 404 (6 U.S.C. Section 204)).

- The scope of this undertaking comprises "the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security." (Homeland Security Act of 2002, as amended – Section 404 (6 U.S.C. Section 204).

- Per its authorizing statute, the Committee is called upon to – and does – "consider risk-based security approaches in the performance of its duties." (Homeland Security Act of 2002, as amended – Section 404 (6 U.S.C. Section 204).

As the details on organization, priorities, and accomplishments that follow in this report thoroughly illustrate, the STSAC is meeting its advisory responsibilities to the TSA Administrator exceptionally well. Simultaneously, the Committee has provided an invaluable coordination forum among leaders in surface transportation in the private sector and state and local government. As a result, the STSAC's voting members have developed and maintained unified positions on priorities for action to enhance transportation security and emergency management and resiliency that have driven cooperative efforts with the Aviation and Maritime Sectors and joint initiatives with TSA, the Department of Transportation (DOT), and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

2) **Meetings of the STSAC and Subcommittees**:

The Committee has met as a whole – voting and non-voting members – on a quarterly basis since the initial organizational session in July 2019. Per the relevant provision of the *TSA Modernization Act of 2018,* at least one session of the full STSAC must be open to the public each year. The dates of the full quarterly STSAC meetings held since completion of the inaugural annual report through the end of 2022 follow – with the public meetings so indicated:

2021	2022
January 25 (ad hoc session)	February 17
February 18	May 12
May 20	August 18
August 19	November 17 – Public
November 18 – Public	December 13 (ad hoc session)

For purposes of meeting the priorities defined by the STSAC, four task-focused subcommittees have been maintained. These subcommittees are staffed by voting members; non-voting members – federal officials with departments and agencies with responsibilities for surface transportation; and, in some cases, invited subject matter experts who bring specific context and insights from experience with issues or activities of interest and concern. During this reporting period, the four subcommittees have cumulatively convened for dozens of virtual meetings – by video call or teleconference. The limitation to virtual sessions resulted from the continuing effects of the COVID-19 pandemic and prudent risk mitigation measures.

Significantly, the areas of emphasis defined by the respective subcommittees illustrate the public-private partnership in action, melding the initiative, perspectives, and priorities of the industry representatives and government officials involved in and leading this collaborative effort. A clear demonstration of this effect is the ready alignment of the outcomes defined in the Administrator's initial tasking letter to the STSAC, dated April 8, 2020, with the subcommittee structure and objectives for action that the voting and non-voting members had already established.

TSA Administrator's Request	STSAC Established Subcommittee
Improving Cybersecurity Information Sharing	Cybersecurity Subcommittee
Addressing Insider Threat	Insider Threat Subcommittee
Measuring Security Effectiveness	Security Risk and Intelligence Subcommittee
COVID-19 Response	Emergency Management and Resiliency Subcommittee
Intelligence and Information Sharing	All Four Subcommittees
Information Protection	All Four Subcommittees

Each week, the elected Chair and Vice Chair of the STSAC hold status calls with TSA's appointed Designated Federal Officer. These consultations focus principally on identifying and resolving or alleviating impediments to the progress of the subcommittees, and the Committee as a whole, in implementation of the approved recommendations.

For a substantial portion of the reporting period, the appointed officers of the respective subcommittees, joined by the elected Chair and Vice Chair, convened to provide status updates to senior surface transportation leadership at TSA. Through these sessions, officers of each subcommittee provided briefings on the progress attained, and impediments encountered, in the collective efforts of the voting and non-voting members to implement the approved recommendations and to advance the Committee's principal purpose of supporting enhancements to security and emergency preparedness across the surface modes of transportation. The level of progress in implementation attained across all four subcommittees enabled termination of these monthly briefs as of the Fall of 2022.

Finally, as an advisory forum for the Administrator, the STSAC's voting members stand ready to provide feedback, insights, and perspective, drawn from assembled expertise and experience representing all surface modes, state and local government, and supporting specializations, on matters of significant concern or interest. The Administrator sought this support when considering actions to address the assessed heightened cyber threat environment during 2021 and 2022, driven notably by the effects of the ransomware attack that targeted Colonial Pipeline in May 2021 and the escalated tensions with Russia over threats against Ukraine in the latter part of 2021 and early 2022 followed by the invasion and ongoing war throughout 2022. During the reporting period, the STSAC:

- Coordinated review and provided feedback on the draft provisions of a proposed Security Directive mandating cybersecurity measures and actions by pipelines. In the latter part of May 2021, following the cyber-attack against Colonial Pipeline earlier that same month, the Administrator had issued an initial Security Directive covering critical pipelines in the United States. During the next two months, the agency drafted a second Security Directive with far more detailed requirements. At the Administrator's request, the STSAC's voting members reviewed the draft provisions and provided unified constructive feedback on alternatives and on proposed revisions.

- As the agency prepared to issue Security Directives on cybersecurity to railroads and rail transit systems in the Fall of 2021, the Committee's voting members reviewed the draft provisions and again provided unified constructive feedback for consideration – on both whether proceeding as planned was necessary and the terms of proposed requirements.

During the public meeting of the STSAC held on November 17, 2022, TSA Surface officials requested the voting members' input on a then pending Advance Notice of Proposed Rulemaking (ANPRM) captioned, *Enhancing Surface Cyber Risk Management*. The agency proposed an ad hoc session of the Committee in early December 2022 – scheduling that would follow the anticipated issuance of the ANPRM in late November. TSA published the ANPRM on November 30. The STSAC feedback session occurred on December 13. A substantial portion of the voting members participated – along with colleagues from TSA and other federal agencies. Comments from Committee members emphasized the critical importance of maintaining a performance-based approach in developing cybersecurity requirements and addressed other priorities and opportunities to enhance the effectiveness of the ANPRM for meeting the intended purpose of guiding the planned rulemaking. Importantly, since this ad hoc STSAC session, the Administrator has reinforced to Committee members the agency's commitment to an outcome and performance-based approach to regulatory action on cybersecurity.

3) **Implementation of the Approved Recommendations to the TSA Administrator**

In official correspondence dated and sent June 30, 2021, the TSA Administrator accepted all of the inaugural recommendations made by the STSAC.

As background, in an ad hoc session of the STSAC held on January 25, 2021, the voting members reviewed and considered each recommendation – and voted on whether to approve or disapprove. The voting members unanimously approved all 18 recommendations – without revisions to content or intended outcomes. Grouped by the sponsoring Subcommittee, the recommendations break out as follows:

- Security Risk and Intelligence Subcommittee: 4 recommendations;
- Cybersecurity Information Sharing Subcommittee: 4 recommendations;
- Insider Threat Subcommittee: 8 recommendations; and
- Emergency Management and Resiliency Subcommittee: 2 recommendations.

By official correspondence dated February 2, 2021, the Committee presented the approved recommendations to the TSA Administrator. In verbal remarks during the public meeting of the STSAC held on May 20, 2021, the Administrator indicated his intent to accept all 18 recommendations. His official correspondence of June 30, 2021, confirmed this decision.

The inaugural 18 recommendations, presented in summary format in the following status review, are grouped under the STSAC subcommittee of principal responsibility for their development, presentation, and coordination and oversight of implementation. The full delineation of the recommendations, similarly organized, and the forwarding memorandum to the TSA Administrator are set out at Appendix B of this report.

Status of Recommendations to the TSA Administrator:

- **Security Risk and Intelligence Subcommittee**:
  - Recommendation #1: Request establishment of a National Intelligence Manager for surface transportation.
    - Status: **In progress**. Thorough and effective efforts initiated by senior surface transportation managers and analysts with TSA Intelligence and Analysis to ensure understanding among key staff leads at DHS's Office of Intelligence and Analysis and the Office of the Director of National Intelligence (DNI) on the purpose and priorities of the STSAC, the need for appointment of a National Intelligence Manager (NIM) for surface transportation, and the preparatory work accomplished within TSA, and through the STSAC, for such an appointment. Awaiting draft for review, feedback, and finalization of the official correspondence from the TSA Administrator asking the DNI to approve the STSAC's request for appointment of a NIM for Surface Transportation as a security priority. The draft will include options for addressing surface industry needs for ODNI advocacy of surface transportation security intelligence requirements.
  - Recommendation #2: Use private sector intelligence requirements to guide federal intelligence collection and inform intelligence analyses and product development.
    - Status: **Implemented – Awaiting Official Closure**. TSA reviewed and catalogued consolidated intelligence requirements for surface transportation based on priorities defined and proposed by representatives of each of the surface modes. These intelligence requirements are being fed into the TSA Intelligence and Analysis Priority Intelligence Requirements development process. The intelligence requirements were submitted to DHS's Office of Intelligence and Analysis, the Office of the Director of National Intelligence (ODNI), and the Department of Transportation (DOT) – with positive feedback on this initiative and its scope and quality.
  - Recommendation #3: Approve and implement the Surface Information Sharing Cell (SISC) charter.
    - Status: **Implemented – Awaiting Official Closure.** The SISC charter has been produced, reviewed, and approved through industry and government participants in the subcommittee and supporting staff elements; and signed by the Transportation Systems Co-Sector Risk Management Agencies (TSA and DOT) and the chairs of the respective surface transportation modal Sector Coordinating Councils (SCCs). Recommendation implemented with the operations of the SISC as an outward-facing element in TSA dedicated to timely sharing of actionable threat intelligence and security information. During the reporting period, the SISC launched the following key initiatives:

        - Twice weekly webinars on cyber and physical security threats, incidents, assessments, and advisories or alerts.
        - Dedicated reference site for the SISC established and regularly updated in the Homeland Security Information Network (HSIN) – with enrollment made available to all members of the STSAC and SISC.
        - TSA Surface Industry Days: Classified briefings on threat intelligence and related security information held on a quarterly basis at TSA headquarters – with participation open to all STSAC and SISC members.
        - Initiated development of DHS HSIN SISC Community of Interest (COI). The purpose of this new COI is to facilitate access for industry and government surface transportation stakeholders with need-to-know to daily unclassified/FOUO intelligence products shared by TSA and other federal and local government stakeholders.

    - Recommendation #4: Complete the Security Risk Methodology Matrix as a resource to support efforts to drive down risk across surface transportation modes.

        - Status: **In progress**. Extensive efforts continue – through the subcommittee's members and TSA subject matter experts, working in coordination with federal interagency security partners – to produce the comprehensive Security Risk Methodology Matrix for surface transportation. The product will support a range of critical activities in industry and government, including risk assessments; exercises – notably scenario development; security planning; defining threat-based alert levels and accompanying protective measures; and action on lessons learned from experience with actual incidents, exercises, and assessments.

- **Cybersecurity Information Sharing Subcommittee**:

    - Recommendation #1: Establish a surface transportation cyber information sharing network on threats, incidents, and security concerns and related alerts, advisories, analyses, and assessments.

        - Status: **In progress**. The establishment of the SISC, as outlined above, provides the essential foundation for implementing this recommendation. Key next steps entail expanding the scope of the SISC's efforts to enable sustained functioning as an information exchange hub for cybersecurity in surface transportation. In this capacity, the SISC will receive, review, and timely disseminate reports submitted by surface transportation entities on actual or potential threats, incidents, and security concerns across surface modes, leveraging existing information sharing forums maintained by each mode. Similarly, the SISC will draw on reporting made to and by the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and through the United States Coast Guard and Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC). The specific aim is to leverage the available reporting and related intelligence and security information on threats, incidents, and significant concerns for prevention and risk mitigation. The SISC will serve a critical role in providing early notification of activity of concern, cyber and physical, for security awareness, informed vigilance, and, as warranted, implementation of protective measures and actions to narrow risk profile and susceptibility across all transportation modes.

- 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.

  - Status: **In progress**. The subcommittee has set clarity on the applicability of the Cybersecurity Information Sharing Act of 2015 as an immediate priority. With TSA's issuance of Security Directives mandating cybersecurity actions and measures by pipelines, rail transit agencies, and railroads, specifically the mandate to report cybersecurity incidents to DHS/CISA, questions have been raised by covered entities on whether sharing through the SISC or established modal information sharing forums remains authorized or permissible.

    Some surface transportation organizations covered by the Security Directives have expressed concern that, once reported to CISA, the information on the cybersecurity incident shifts to government control and, therefore, only government can act to disseminate further. In similar vein, other surface transportation entities covered by the TSA directives have expressed reservations about sharing information on activity of interest not reported to CISA with colleagues in their respective industries and across modes and sectors. Their concern is the prospect of review of shared information not reported to CISA to determine whether noncompliance with the terms of the applicable Security Directive has occurred.

    TSA participants in the subcommittee have consulted with attorneys at the agency's Office of Chief Counsel for advice and guidance on interpretations of the 2015 statute in the context of the reporting mandated in the Security Directives. TSA Surface Policy staff is engaged as well in a concerted effort to clarify interpretation and understanding and resolve the cited concerns.

- Recommendation #3: Establish effective procedures for broad sharing of cyber threat and security information across surface transportation modes, leveraging proven means already in place through industry initiatives.

  - Status: **In progress**. Full implementation is dependent upon the expansion in functioning of the SISC to serve as the information exchange hub – from industry to government and government to industry – for reporting and for timely sharing of reporting, analyses, and assessments on cyber threats, incidents, and significant security concerns. Once attained, each of the surface modes has long-established and proven information sharing forums to ensure reports of significant security concerns, cyber and physical, and related alerts, advisories, analyses, or notifications reach the right recipients to inform vigilance and appropriate security actions and measures for prevention and risk mitigation.

- Recommendation #4: Conduct an annual review to assess the performance and impact of the Surface Information Sharing Cell (SISC).
  - Status: **In progress**. As outlined above, the SISC is progressively building toward functioning at the planned capacity to meet the recommendations to the Administrator on cybersecurity information sharing. The evaluation of the SISC's effectiveness will commence within one year of its implementing this expanded role for cyber threat awareness, informed vigilance, and risk mitigation through timely sharing of actionable intelligence and related security information. Meanwhile, the subcommittee is developing proposed parameters for the annual evaluation of the SISC – for which feedback from the broader STSAC membership will be sought.

- **Insider Threat Subcommittee**:
  - 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.
    - Status: **In progress**. The Insider Risk Mitigation Hub (IRMH) is currently operational. The Hub is a comprehensive resource for government and industry usage in expanding capabilities to detect, deter, and disrupt potential insider threat activity. Staff members within TSA responsible for this program are working diligently to elevate the hub to full operational capability. In a substantial demonstration of progress and commitment, TSA has secured funding for program development support. The initial scope of this initiative entailed assessing the current Hub. Further work continues, focused on assessing stakeholder integration in the near term and maturing and professionalizing the IRMH over the next few years by identifying areas for improvement and reporting. Full implementation with industry participation is projected by September 2023.
  - 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.
    - Status: **Implemented – Awaiting Official Closure**. The Case Optimization and Risk Evaluation (CORE) tool is an analytics suite within the Insider Threat Case Management System. Data migration was completed on November 14, 2022, and the system is currently being validated and reviewed before final rollout.

      The Insider Threat Case Management System (CMS) completed the agile development process as of November 2, 2022. The CORE Tool was concurrently developed to act as the analytic capability for prioritizing and evaluating risk information within the system. Developers are currently assisting with the migration of legacy data, which will be followed by rollout of the system – projected to occur during the first half of 2023.

- Recommendation #3: Implement a nationwide online tip capability providing a timely and simple means to report suspicious activity and threats for surface transportation organizations lacking effective procedures for reporting significant security concerns.
    - Status: **Implemented – Awaiting Official Closure**. Well-conceived and functioning reporting procedures are in place in many organizations across surface modes. There is no intent to co-opt, duplicate, undermine, or upset these proven effective practices. However, some surface transportation entities lack this advantage. The recommendation on the "tipline" is intended to fill gaps of this kind, while also providing an option for the public at large to report suspicious activity and other security concerns in surface transportation.

      With this initiative, the Insider Threat Subcommittee has focused on leveraging an existing capability and expanding on it – to enable and expedite effective implementation and progressively build confidence in reliability as an effective means for both reporting and facilitating timely analysis. Work for these purposes has included a survey that sought input from all STSAC members in the latter part of 2021 and early 2022. This outreach highlighted the importance of integrating a reporting capability with TSA's Freedom Center, also known as the Transportation Security Operations Center (TSOC), to simplify the process for prospective users – whether in the public at large or workers at a surface transportation entity that lacks consistent and effective reporting procedures – and ease review to identify patterns, trends, and indicators of concern or their absence.

      In accordance with policy and national standards, the TSA Insider Threat Program (ITP) has created – and is currently utilizing – a mechanism for the intake and processing of reports of suspicious activity and threats for surface transportation organizations via a telephone "hotline" and an email inbox. Reports on matters implicating insider threat concerns are subsequently entered into the Insider Threat Case Management System (ITCMS) for tracking and adjudication within the Insider Threat Risk Mitigation Hub (IRMH). Significantly, the TSA Insider Threat Program continues to expand outreach efforts across the surface, aviation, and maritime transportation systems in order to increase awareness of and reporting on potential insider threats. A complementary initiative is bolstering the capacity to receive reports and enter them for assessment and analysis – notably by integration with the TSA Contact Center (TCC), which assures the needed capability to handle the volume of telephonic and written reports and enter relevant information for case review and analysis.

- Recommendation #4: Define parameters for assessing the level of potential insider threat risk posed to organizations in the surface transportation modes.
  - Status: **Temporary hiatus**. The subcommittee's aim with this recommendation is to categorize positions in surface transportation based on potential risk factors for insider threat, particularly through distinguishing employees, contractors, and third-party suppliers or service providers that perform security sensitive functions or access sensitive areas from other types of workers. In a supporting initiative, the subcommittee has planned to develop a matrix of public sector and private industry workforce vetting programs and their respective functional elements as a resource for the surface transportation community, industry and government.

    Due to TSA's planned issuance of a notice of proposed rulemaking (NPRM) on security vetting of surface transportation workers, efforts to implement this recommendation have paused temporarily. The subcommittee seeks to ensure that its work in defining parameters that surface transportation organizations can adopt and apply for assessing insider threat risk complements and informs, as opposed to conflicts with or detracts from, the anticipated rulemaking initiative.

- 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.
  - Status: **Temporary hiatus**. This recommendation constitutes the practical application of the outcomes attained in implementing its immediate predecessor, Recommendation 4. The development of the matrix of public sector and private industry workforce vetting programs facilitates the identification of effective practices that surface transportation organizations can adopt and adapt for conducting background checks of employees, contractors, and suppliers and service providers. Effectiveness and sustainability are boosted by application of risk-based factors to determine the level of security risk associated with positions and access.

    Again, though, due to TSA's planned issuance of the NPRM on security vetting of surface transportation workers, efforts toward implementing this recommendation have paused temporarily. Significantly, however, the subcommittee's work in developing and identifying effective practices for risk-based categorizations of responsibilities, functions, and access to determine the type and scope of vetting can complement and inform the anticipated rulemaking initiative.

- Recommendation #6: Expand the scope of participation in TSA's existing Insider Threat Executive Steering Committee by including representatives of the STSAC and Aviation Security Advisory Committee (ASAC).
  - Status: **Implemented – Awaiting Official Closure**. Significantly, the Administrator accepted this recommendation with the stipulation that its implementation aligns with the approach on a similar priority set by the ASAC. Specifically, TSA's "Insider Threat Executive Steering Committee (ESC) is an internal body whose purpose is to provide strategic direction."

    The STSAC's objective in approving this recommendation is to gain a consistent and effective voice for surface transportation security priorities with TSA's Insider Threat Executive Steering Committee. To achieve this purpose, there is no need to change the status or composition of the steering committee. Rather, the aim is to assure recurring opportunities for representatives of the STSAC's voting members to meet with TSA's executive leadership to present concerns, address and shape priorities, and provide and gain insights on the development of programs, resources, and related initiatives for insider threat awareness and risk mitigation.

    This recommendation has been implemented to accomplish these outcomes. TSA officials who serve as Government Co-Chairs of the subcommittee are among the members of the agency's Insider Threat Executive Steering Committee. In this dual capacity, they are well informed and positioned to present the principal concerns and driving priorities of the subcommittee for insider threat risk mitigation. Further, members of the STSAC's Insider Threat Subcommittee, and their counterparts with the ASAC, will be invited on a recurring basis to provide updates on progress in their respective areas and briefings on priorities and concerns, as necessary. Subcommittee members will also be consulted on matters that implicate their work to enhance capabilities and support for mitigation of insider threat risk for organizations across the surface modes of transportation. TSA's executive leadership is fully committed to this approach – with particular emphasis on the critical importance of continued dialog to ensure the intent and purpose of this recommendation continue to be met.

- Recommendation #7: Establish a consistent process to facilitate communication by federal agencies to transportation organizations of sensitive information on reports or allegations of terrorist or extremist ties, or suspected illicit insider activity, on workers.
  - Status: **In progress**. Proper scoping of this recommendation is critical to its implementation and sustained effectiveness for meeting its intended purpose. The outcome sought is a consistent practice by which federal authorities can apprise surface transportation organizations of sensitive information concerning an employee, contractor, or on-site supplier or service provider for whom terrorist watchlist vetting has produced a presumed match or an

investigation has been initiated for suspected actions that create or indicate an escalated insider threat risk. At present, there is neither clarity nor consistency on whether notifications are made, to whom they are conveyed in an affected organization, and by what means.

The overarching importance of avoiding any course of action that prejudices the conduct of an ongoing investigation, especially when driven by the prospect of connections to terrorists or extremists, is understood and respected. At the same time, however, regard must be accorded to the chief of police or the security lead for a surface transportation organization who is responsible for assuring worker and public safety.

A viable solution is the recognition of police chiefs and security leads for surface transportation organizations – who hold security clearances awarded and maintained by federal government departments and agencies – as identified, and verified, trusted agents for receipt or discussion of this type of sensitive information. The subcommittee is pursuing development of guidelines to support implementation of a clear and consistent communications process.

- Recommendation #8: Maintain a consolidated insider threat information resource for transportation on the Homeland Security Information Network (HSIN).
    - Status: **In progress**. From the latter part of 2021 through the Fall of 2022, the subcommittee dedicated extensive efforts to defining and attaining this priority. This work included:
        - Within the subcommittee and in consultations with subject matter experts on insider threats and risk mitigation, developing concepts and objectives for a resource site, determining the most effective platform to host, assembling relevant materials and reference sources, and engaging expertise in site design and maintenance.
        - Beyond the subcommittee, consultations and coordinated and cooperative efforts with and among multiple federal government agencies, most notably DHS/CISA, to enable the establishment of a site focused principally on the insider threat to surface transportation on the Homeland Security Information Network (HSIN) for access by government officials and industry stakeholders.
        - A joint effort linking subcommittee members with technical experts in design and management for HSIN produced test sites for usage by and feedback from experienced government officials and industry stakeholders – on appearance and functioning, on assembled materials, and on the value and utility of the consolidation of information.
        - Integration of recommendations from participants in these initial pilot tests to enhance the accessibility and functioning of this developing capability.

- For the meeting of the STSAC held in August 2022, the subcommittee devoted the full period of time allotted for its update to demonstrate the site. This presentation covered five topics:
    - Build Your Insider Threat Program;
    - Insider Threat Quick Reference Material;
    - Insider Threat Intelligence Products;
    - Insider Threat Best Practices and Reports; and
    - Insider Threat Training, Case Studies, and Reference Links.
- Following this meeting, the subcommittee opened the test site for access, review, and feedback from all members of and participants in the STSAC.
- Developers integrated constructive input received in this second phase of pilot testing for further enhancements to the site's appearance, features, functioning, and types of materials maintained.
- The result: In advance of the STSAC's public meeting, held in November 2022, the planned Surface Transportation Insider Threat Library had been opened for access to Committee members.
- Next steps: Complete the assembling and production of content for the library; define and implement needed quality control measures; and activate the site for general access.

Too often, the challenge that practitioners in homeland security face is not a dearth of relevant reports, analyses, assessments, advisories, and other reference materials, but rather a plethora, spread widely across numerous websites maintained by government departments and agencies and private sector organizations. The HSIN Surface Transportation Insider Threat Library has been developed specifically to alleviate this problem. The effort devoted to consolidation yields immediate and long-term positive impacts. Burdens are eased substantially on hard-pressed security directors or insider threat program managers seeking resources to meet their responsibilities and keep plans, programs, and related risk mitigation initiatives current and vibrant. As a representative example, a surface transportation organization's security lead or chief of police could consult the HSIN Surface Transportation Insider Threat Library to obtain helpful materials readily for awareness training of employees on indicators of concern based on experience with actual incidents.

The eight recommendations produced by this subcommittee aim to produce integrated solutions for mitigating insider threat risk in organizations across the surface modes of transportation.

- Recommendation 6 on engagement with TSA's Insider Threat Executive Steering Committee sets a structured approach, fully supported by the agency, for sustained consultations to foster coordinated efforts by government and industry on insider risk mitigation priorities, programs, and initiatives.

- In similar vein, Recommendation 7 seeks to establish a general clarity and consistency for communication by federal authorities with security or law enforcement leads of surface transportation entities on investigative activities directed at a worker for suspected or indicated terrorist or extremist ties or alleged actions or statements implicating concern with insider threat risk.

- Recommendations 4 and 5 focus on risk-based assessments and effective practices for insider risk mitigation – efforts that can inform determinations pertinent for TSA's consideration in the planned rulemaking on security vetting of surface transportation workers.
- Finally, the remaining recommendations – the Insider Risk Mitigation Hub (Recommendation 1); the Case Optimization Risk Evaluation tool (Recommendation 2); the voice/email/text "tipline" for entities that lack standing procedures for reporting (Recommendation 3); and the HSIN Surface Transportation Insider Threat Library (Recommendation 8) – collectively strive to assemble resources and develop capabilities that organizations in each of the surface modes can leverage thoroughly and effectively in programs and initiatives focused on insider threat awareness, early detection for prevention, timely reporting of indicators of concern, and overall risk mitigation.

Those responsible for security and law enforcement in surface transportation organizations, seeking to detect and prevent threats and incidents, often ask, "What signs or indicators of the developing insider threat seemed to occur over and over again in incidents in transportation entities?" The work of this subcommittee is focused on ensuring accessible, comprehensive, and practically applicable means are in place for a productive response based on case analyses.

- **Emergency Management and Resiliency**:
    - ▪ Recommendation #1: Enhance pandemic preparedness by sharing lessons learned on response to COVID-19 across modes.
        - o Status: **Fully Implemented**. The subcommittee held two focused and well attended workshops on responses by surface transportation organizations to the pandemic – with emphases on what worked well, what did not, and lessons learned that may be applied and adapted to enhance preparedness for future events of this scope and impact. The results have been captured in two concise information briefs that have been disseminated and posted widely to facilitate access.

          Significantly, this subcommittee did not result from the Administrator's tasking letter to the STSAC in April 2020. The Committee's voting members proposed forming a group focused on emergency preparedness, incident management, and resiliency of surface transportation operations. The foresight of this decision and action in establishing the Emergency Management and Resiliency Subcommittee manifested dramatically with the onset and highly disruptive effects caused by the pandemic.

          The two workshops enabled surface transportation professionals to share practical experiences in responding to and seeking to ameliorate the unique impediments, challenges, and stress factors imposed by the rapid and sustained spread of the virus in successive waves. The first session took place at the height of the disruptive and, in some cases, debilitating effects of the pandemic, serving essentially as an in-progress review of the scale of adverse impacts on surface transportation workforces, passengers, and operations and of measures taken to maintain a reasonable level of resiliency as critical infrastructure. The subcommittee held the second workshop when pandemic impacts had begun to recede. As a result, this session afforded the opportunity to focus attention on how surface transportation organizations adjusted response actions and measures to mitigate pandemic effects and began to prepare for returns to facilities, expansions in ridership, and increased interaction with workers in other sectors as lockdowns and restrictions on activity were progressively relaxed.

Difficulties encountered by surface transportation organizations with workers and passengers in meeting the requirements of TSA Security Directives that mandated the wearing of face masks presented principal issues of concern and areas of extensive discussions in both phases. Insights gleaned based on the experiences, challenges, and impediments that surface transportation organizations encountered provides a resource to inform and guide decision-making and actions on whether such directives are the most effective way to attain risk mitigation in future efforts to stem spread of highly contagious and serious illnesses in public settings.

- Recommendation #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.
  - Status: **Fully Implemented**. The subcommittee has established a standing procedure for recurring review and update, as warranted, of its concise reports on effective practices and lessons learned from the two workshops held on responses and enhancements to preparedness actions and measures taken by surface transportation organizations during the COVID-19 pandemic. The specific purpose is to ensure the information assembled remains accurate, relevant, and actionable as guides for decision-making and implementing actions.

As the first subcommittee to complete implementation of its approved recommendations, the Emergency Management and Resiliency Subcommittee did initiate consideration of subject areas for future recommendations during the latter part of 2022. A priority identified for attention is the potential impacts that could result to the surface transportation community in the event of a disruption to the power grid in light of transitions to electric or cleaner technology vehicles. Consistent with the effective practice developed and demonstrated to review response actions and measures taken by surface transportation organizations to address the effects of the COVID-19 pandemic, the subcommittee will sponsor, plan and prepare for, and conduct a workshop focused on identifying and addressing the challenges and opportunities implicated by transitions to electric vehicle fleets by surface transportation entities.

4) **Look Ahead to 2023 – Initial Priorities and Objectives**:

Full Committee: Building on the opportunities extended in 2021 and 2022 to voting members to provide feedback on security mandates under consideration by TSA, the STSAC will consider options to institutionalize this effective practice. These may include establishing a dedicated forum to facilitate these types of consultations – such as through a new Security Requirements Subcommittee, which TSA senior executives had proposed in 2021; integration of this role in the scope of the existing subcommittees; or a combination of these options. The intention is to afford the Administrator with a dedicated process whose specific purpose is coordination of timely review, feedback on, and discussions of proposed directives or rulemaking initiatives. Consultations among the voting members on these options will occur in conjunction with a quarterly meeting of the full Committee in 2023.

Security Risk and Intelligence Subcommittee:

- Seek and develop engagement with ODNI National Intelligence Managers (NIMs) with critical infrastructure security portfolios to explore a potential NIM advocate/champion for surface transportation intelligence requirements. Complete drafting of and coordination on the official correspondence from the TSA Administrator, on behalf of the STSAC, to the Director of National Intelligence (DNI) seeking appointment of a National Intelligence Manager for Surface Transportation or a similar NIM advocate for surface transportation security intelligence requirements.
- In coordination with TSA and the Transportation Systems Sector (TSS) Government Coordinating Council (GCC) and Sector Coordinating Councils (SCC), finalize the prerequisites for applicants and the procedures for review and approval of requests to join the Surface Information Sharing Cell (SISC).
- Launch new DHS HSIN/SISC Community of Interest (COI). This new COI will give thousands of private industry and government surface transportation stakeholders with a need-to-know access to daily unclassified/FOUO intelligence products shared by TSA and other federal and local government stakeholders.
- Propose for consideration the establishment of remote connections, as capabilities via secure video-teleconference or secure phone permit, for participation in the quarterly TSA Surface Industry Day classified briefings and discussions on threats, incidents, and significant security concerns, physical and cyber.

Cybersecurity Information Sharing Subcommittee:

- Detail the actions necessary to expand the scope of the SISC's efforts to enable sustained functioning as an information exchange hub for cybersecurity in surface transportation. Specifically, how the SISC will receive, review, and timely disseminate reports submitted by surface transportation entities on actual or potential threats, incidents, and security concerns across surface modes, leveraging existing information sharing procedures maintained by each mode.

- Coordinate with TSA Surface Policy to develop guidance clarifying the applicability of the Cybersecurity Information Sharing Act of 2015 to reporting of cybersecurity incidents by surface transportation organizations covered by the agency's Security Directives mandating cybersecurity measures and actions. Specifically, this guidance is intended to facilitate expanded cybersecurity information sharing – by clarifying that (1) information in reports made to DHS/CISA under the applicable Security Directive may be shared by the reporting organization with partners in its mode of transportation and colleagues in other modes and critical infrastructure sectors; and (2) information shared within an industry or across modes and sectors is not being, and will not be, scrutinized by either TSA or CISA to determine if a report on the same matter should have been made pursuant to an applicable Security Directive.
- Draft parameters for evaluation of the SISC's effectiveness in cybersecurity information sharing. This action is dependent upon the SISC achieving sustained functioning as an information exchange hub for cybersecurity in surface transportation.

Insider Threat Subcommittee:

- Elevate the Insider Risk Management Hub (IRMH) to full implementation by integrating industry participation.
- Determine feasibility of options to implement the "tipline" reporting capability, in voice, email, and text formats, integrated with the Surface Watch at TSA's Freedom Center – as an option for surface transportation organizations that lack standing procedures and capacity for reporting observed or encountered significant security concerns to TSA.
- Resume work on Recommendations 4 and 5 on assessing and categorizing insider threat risk based on surface transportation workers' responsibilities and levels of access; and on defining risk-based priorities and effective practices for vetting of workers – again when warranted by the nature of their responsibilities and levels of access. With the expertise and experience assembled in the STSAC, and the track record of discretion and attention to detail brought to all tasks, this work will yield insights and considerations to inform TSA's determinations on whether a rulemaking on security vetting is necessary and, if so, how any proposed requirements address risk-based priorities for insider threat mitigation.
- Propose a consistent process to facilitate communication by federal agencies to transportation organizations of sensitive information on reports or allegations of terrorist or extremist ties, or suspected illicit insider activity, on surface transportation workers.

Emergency Management and Resiliency Subcommittee:

- Hold the workshop on "potential impacts that could result to the surface transportation community in the event of a disruption to the power grid in light of transitions to cleaner technology." This event is scheduled for Wednesday, March 15, 2023, from 1:00 to 3:00 pm Eastern standard time. Subjects to be covered include: Energy Sector and Power Grid Overview; Unclassified Intelligence Briefing (power grid); Industry Perspectives; and Open Discussion. Participants will represent surface transportation organizations, supporting industry associations, officials with federal government departments and agencies, and other interested parties. Projected outcome is an information brief focused on key findings, identified gaps and concerns, solutions already in place or in development that can be leveraged, and recommendations on priorities for preparedness.

- As a tool to support emergency management professionals in surface transportation organizations, the subcommittee will work with TSA's HSIN technical support team to develop a comprehensive library of resources on preparedness, incident management, and assuring operational resilience in surface transportation – in all hazards emergency conditions. Similar to the Insider Threat Subcommittee's initiative on its HSIN Surface Transportation Insider Threat Library, the aim is to ease burdens on emergency management leads and first responders in surface transportation organizations by consolidating, at a readily accessible site, the wide range of reference materials currently maintained separately across numerous platforms administered by government departments and agencies, industry associations, centers of excellence, academic institutions, and private sector entities.

- Through consultations within the subcommittee and with colleagues in the full Committee, federal government officials, and subject matter experts, continue to review opportunities for development of new recommendations to enhance capabilities and support for emergency preparedness, incident management, and operational resiliency.

5) **Acknowledgments**:

The Chair and Vice Chair commend all members of the Surface Transportation Security Advisory Committee (STSAC) – industry and government. The progress attained in implementing the approved recommendations and the foundation set for more are impressive – especially when considered in the context of the demands that industry representatives and government officials have faced throughout the extended period covered by this report.

We recognize, and respect, that the level of commitment of time and effort to enable this scale of progress is substantial. Given the unrelenting demands of full-time positions, much of the work on STSAC priorities inevitably consumes nights, weekends, and even time off. It is commonplace for members – in industry and government – to join meetings remotely while on vacation or addressing personal or family concerns. Words alone cannot adequately express our gratitude for the collective dedication demonstrated by all involved in the work of this Committee.

Meriting commendation as well are the Administrator, senior executives, and supporting staff at TSA. We often refer to the work of this Committee as illustrative of the public-private partnership in action. Leadership is the pillar of an effective partnership. The Administrator and his team provide that essential foundation – not simply through acceptance of the STSAC's recommendations, but also by actions that make them attainable, including, most notably, commitments of personnel and resources. In this vein, we gratefully acknowledge the exceptional support provided by executive and policy leads at TSA, including Stacey Fitzmaurice, Eddie Mayenschein, Kristin Simonds, Sonya Proctor, Scott Gorton, David Cooper, Judith Harroun-Lord, and Felicia Valois – as well as others whose work behind the scenes ensures that meetings are well planned and conducted, deliberations and decisions and actions accurately and thoroughly documented, and conditions fostered to support progress and success.

Further, we extend sincere appreciation to Steve Alterman and Chris Bidwell, respectively the Chair and Vice Chair of the Aviation Security Advisory Committee (ASAC), for their cooperation and support of our shared purpose of enhancing security and emergency preparedness. Steve and Chris are regular participants in STSAC meetings – a courtesy they extend as well for ASAC sessions to the Chair and Vice Chair of the STSAC. Their openness to sharing insights and lessons gained from experience in managing a similar forum for the Aviation Sector has continuously proven invaluable. These connections have shown their worth repeatedly in the unprecedented challenges confronted and opportunities created during the past three years.

Finally, as alluded to in the expression of appreciation for support from TSA leadership and staff, work of the caliber reflected in this report simply cannot happen without assistance provided from many quarters. Likely we will never know their names or what they have done and sacrificed. They are colleagues at work or family members at home. Unquestionably, their selflessness makes differences for the members of the STSAC. For, whether representing industry or government, they are better able to prepare for, participate in, and contribute to informed dialogue at recurring subcommittee teleconferences and webinars, full Committee meetings, and ad hoc sessions and to complete work on defined priorities for action to implement recommendations and produce positive outcomes for surface transportation security and emergency preparedness. To this extensive group of unseen supporters, we extend a collective, and humble, “Thank you!”

6) **Appendices**:

- Appendix A: STSAC – Timeline of Activities (2021 – 2022)
- Appendix B: Unanimously Approved STSAC Recommendations to TSA Administrator

Respectfully submitted,

Thomas L. Farmer

Thomas L. Farmer
Chair – STSAC
Assistant Vice President – Security
Association of American Railroads

Polly L. Hanson
Vice Chair - STSAC
Director, Security, Risk and Emergency Mgt.
American Public Transportation Association

Appendix A: Surface Transportation Security Advisory Committee (STSAC) Timeline (2021 – 2022)

- **January 25, 2021**: Ad hoc session of the STSAC of voting and non-voting members for the purpose of reviewing, discussing, and voting to approve or disapprove the inaugural recommendations to the TSA Administrator to enhance security, critical infrastructure protection, emergency preparedness, and operational resiliency in the surface transportation modes. Each of the four subcommittees offered its recommendations for review, discussion, and consideration. A total of 18 recommendations were made – as follows: Security Risk and Intelligence (4); Cybersecurity Information Sharing (4); Insider Threat (8); and Emergency Management and Resiliency (2). In the voting, the STSAC's voting members unanimously approved all 18 recommendations.

- **February 2, 2021**: The STSAC submitted the 18 unanimously approved recommendations to the Administrator of the Transportation Security Administration (TSA).

- **February 18, 2021**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic.

- **April 1, 2021**: First annual report of the STSAC submitted to TSA for presentation to the Administrator and for delivery to the appropriate Congressional committees. This inaugural report covered the period from the Committee's inception through March 31, 2021 – with the extension into 2021 made to ensure coverage of the unanimous approval by the voting members of the 18 recommendations and their formal submission to the Administrator.

- **May 20, 2021**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic. In remarks to the voting and non-voting members, the TSA Administrator indicated his acceptance of the STSAC's 18 unanimously approved recommendations. Official correspondence ratifying this acceptance to follow.

- **June 30, 2021**: Official correspondence from the TSA Administrator to the STSAC confirms acceptance of all 18 unanimously approved recommendations.

- **August 19, 2021**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic.

- **November 18, 2021**: STSAC public meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic. The TSA Administrator, senior TSA executives who serve in or support the Committee, and the Chair and Vice Chair of the STSAC welcomed six newly appointed voting members.

- **February 17, 2022**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic.

- **May 12, 2022**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic.

- **June 17, 2022**: Via Federal Register notice, TSA published a request for "applications from individuals who are interested in being appointed to serve on the Surface Transportation Security Advisory Committee (STSAC)." The notice specified relevant qualifications and representation of a surface transportation constituency that prospective applicants are required to meet. Positions on the Committee open for new appointment or reappointment were those for which the incumbents had been appointed more than 2 years previously. Applications were accepted through the set deadline of July 18, 2022.

- **August 18, 2022**: STSAC meeting – held fully virtually due to the continuing effects of the COVID-19 pandemic.

- **October 24, 2022**: TSA Administrator David Pekoske holds a "meet and greet" webinar with the newly appointed and reappointed members of the STSAC. After thorough review of applications, the Administrator reappointed 12 voting members to a new term of service and selected 13 new members. The positions of eight voting members were not open for appointment – as they had not yet served the initial term of at least two years. With these appointments, the Committee is now comprised of 33 voting members. Collectively, these decisions and actions by the Administrator have initiated a standard approach for reviewing, and renewing, STSAC membership on a recurring, and consistent, basis.

- **November 17, 2022**: STSAC public meeting – hybrid session. For the first time since the first quarter meeting in January 2020, the Committee convened partly in-person – hosted at TSA's new headquarters facility in Springfield, Virginia. The TSA Administrator, senior TSA executives who serve in or support the Committee, and the Chair and Vice Chair of the STSAC welcomed the 13 newly appointed voting members and the 12 reappointed voting members.

- **December 8, 2022**: Ad hoc session held with the voting members of the STSAC – with participation by federal government officials from TSA and other interested departments and agencies – for constructive feedback on the advance notice of proposed rulemaking (ANPRM) captioned *Enhancing Surface Cyber Risk Management*, published on November 30, 2022.

Appendix B: STSAC's Unanimously Approved Recommendations to the Administrator

Surface Transportation Security Advisory Committee (STSAC)
Approved Fiscal Year 2021 (FY2021) Recommendations
for the
Administrator of the Transportation Security Administration (TSA)

February 2, 2021

Security Risk and Intelligence:

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.

Cybersecurity Information Sharing:

STSAC Cybersecurity Information Sharing 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 Information Sharing 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 Information Sharing 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 Information Sharing 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.

Insider Threat:

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 Aviation Security Advisory Committee (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.

<u>Emergency Management and Resiliency</u>:

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.