BEFORE THE
TRANSPORTATION SECURITY ADMINISTRATION
DEPARTMENT OF HOMELAND SECURITY

TSA–2022–0001

ENHANCING SURFACE CYBER RISK MANAGEMENT

COMMENTS OF THE ASSOCIATION OF AMERICAN RAILROADS AND THE AMERICAN SHORT LINE AND REGIONAL RAILROAD ASSOCIATION

The Association of American Railroads ("AAR") and the American Short Line and Regional Railroad Association ("ASLRRA") respectfully submit these comments in response to the advance notice of proposed rulemaking ("ANPRM") issued by the Transportation Security Administration ("TSA").[1] The ANPRM requests input regarding "how the pipeline and rail sectors implement cyber risk management ("CRM") in their operations and will support us in achieving objectives related to the enhancement of pipeline and rail cybersecurity."[2] These comments first set forth general comments and principles that should be followed throughout the process, then provide responses, to the extent appropriate, in the specific topic areas.

Background

AAR freight railroad members include the seven U.S. Class I railroads, as well as scores of U.S. short line and regional railroads. Collectively, these carriers account for the vast

[1] TSA, Enhancing Surface Cyber Risk Management, Advanced Notice of Proposed Rulemaking (Nov. 30, 2022) ("ANPRM").

[2] *Id.* at 73527.

majority of freight railroad mileage, employees, and traffic in the United States. Together with their Mexican and Canadian counterparts, U.S. freight railroads form an integrated, continent-wide network that provides the world's best freight rail service. In addition, the AAR's passenger railroad members, which include Amtrak and various commuter railroads, account for more than 80 percent of U.S. passenger railroad trips.

ASLRRA represents the short line railroad industry, comprised of 603 Class II and III line railroads, many switching operations, and the suppliers that serve them. An average short line is about 70 miles long with approximately 18 employees serving about a dozen local customers. Class II and III Railroads in total support 478,820 jobs, $26.1 billion in labor income, and $56.2 billion in value-add to the economy, playing a particularly large role in the agricultural, manufacturing, and energy industries. Importantly, ASLRRA members provide the first- and last-mile connections for local areas connecting manufacturers, businesses and farmers in communities and small towns to larger markets, urban centers, and ports.

This diverse group of AAR and ASLRRA members has been at the forefront of cybersecurity in the Transportation Sector since the turn of the century. Railroads operate 24-hours per day, seven days a week, and focus continuously on the safety and security of those operations. For more than 20 years, railroads have maintained a dedicated coordinating committee focused on cyber threats, incidents, and indicators of concern; effective risk mitigation practices; and engagement with government agencies like the Department of Homeland Security ("DHS"), TSA, the National Security Agency, and, in more recent years, the Cybersecurity and Infrastructure Security Agency ("CISA"). By tapping into this robust range of private and public capabilities, railroads are, and have been, prepared to prevent and respond effectively to malicious cyber activity. The changing threat environment demands that private and public entities' response capabilities remain flexible, nimble, and sustainable.

As TSA is well-aware, a majority of AAR members and a significant number of ASLRRA members are subject to TSA's security directives on cybersecurity, including SD 1580-21-01 and SD 1582-21-01 ("first SD") and SD 1580/82-2022-01 ("second SD") (collectively "SDs"). The industry's experience with the SDs has also helped in shaping and guiding the preparation of these comments. AAR and ASLRRA look forward to engaging further as the process progresses.

General Comments

I. History of Rail Industry Cyber Security Programs

Railroads have prioritized cybersecurity since before the turn of the century, including how to mitigate against cyber risk. Through a dedicated forum – the Rail Information Security Committee ("RISC") established in 1999 – railroads share information on significant cyber threats, incidents, and indicators of cybersecurity concern and effective risk mitigation practices to inform vigilance and elevate security posture industry-wide. As an effective practice, sustained over numerous years, railroads have conducted recurring assessments of cybersecurity risk and acted on results in a continuous improvement process. Through these assessments, railroads have identified critical cyber functions, evaluated their cybersecurity posture in the context of prevailing and evolving threats, and prioritized actions, measures, and controls to mitigate the risk of disruption to operations assuring resiliency. These sustained efforts have met priorities defined in the National Institute of Standards and Technology ("NIST") Cyber Security Framework as well as strong recommendations by TSA and CISA.

In addition, as an after-action priority identified during the first cross-modal cybersecurity tabletop exercise held by TSA in August 2014, the railroad industry proposed establishing an early notification network for cyber threats, incidents, and significant security concerns. The concept envisioned TSA serving as a coordination point for cybersecurity information sharing among organizations across all modes. Through the Railway Alert Network ("RAN"), the railroad industry turned the concept into practice, implementing a standard process for timely sharing of cybersecurity advisories and awareness messages based on reporting by railroads and supporting industry organizations and with government agencies, including TSA, CISA, the Federal Bureau of Investigation ("FBI"), the Department of Transportation, Department of Defense ("DoD") commands, and Transport Canada. Significantly, in early 2021, this sustained practice became the impetus for a recommendation by the Congressionally mandated Surface Transportation Security Advisory Committee ("STSAC") to the TSA Administrator on cybersecurity information sharing. Specifically, the STSAC recommended TSA should maintain its Surface Information Sharing Cell as a "hub" for disseminating alerts, advisories, and reports of threats, incidents, and security concerns through the "spokes" of modal information sharing networks to transportation entities across all modes.

In the weeks following the Colonial Pipeline ransomware incident in May 2021, the railroad industry joined the Mass Transit Sector in proposing a comprehensive strategy for joint government and industry action to mitigate cybersecurity risk in the Transportation Sector. In June and July 2021, teleconferences were held with TSA during which the concepts for a proposed joint strategy were discussed. In August 2021, well before the announced intention to issue a security directive for railroads and rail transit systems, representatives of the Rail Sector and Mass Transit Sector presented the proposed strategy to TSA for consideration, review, and feedback. The strategy's provisions mark the first concerted effort to apply the TSA's Cybersecurity Road Map for the Transportation Sector issued in 2018. While no official response has been provided, industry remains committed to this type of unified approach to cybersecurity risk mitigation under the auspices of the public-private partnership.

These proactive and extensive efforts by railroads to develop, implement, and continuously improve plans, practices, and measures for cybersecurity as threats and security concerns emerge have assured resiliency of operations. Cybersecurity is always evolving, and real-time adaptation is essential to reduce risk. AAR and ASLRRA believe regulation is not required, particularly considering the extensive efforts of the industry to mitigate risk, and the ongoing implementation of the SDs by industry. Experience and lessons learned with this implementation, as well as inspections and ongoing consultations between agency officials and industry representatives, are likely to offer several lessons for rail operators and TSA that make further rulemaking premature at this time. If TSA does propose a rule, it must consider the necessity of any prescribed requirements and the appropriate scope of implementation through the lens of the recurring risk assessments that railroads already conduct and the effective cybersecurity practices already in effect – long-maintained and continuously evaluated for enhancement.

II. Performance-Based and Risk-Based Regulations

The railroad industry's demonstrated commitment to cyber-readiness and risk mitigation merit strong consideration when determining whether there is a need for TSA regulations. Based on the extensive and sustained efforts dedicated to elevating rail operators' cybersecurity posture, maintained for more than two decades, the industry does not agree that regulations are necessary. This track record of leadership is evidence of the incentives already in place for the railroads to reduce cyber risk. TSA and DHS should not rush to regulate, particularly while DHS is separately promoting Cross-Sector Cybersecurity Performance Goals ("CPGs"), which by Presidential National Security Memorandum are expected to be customized for each sector of critical infrastructure.[3] This suggests an unfortunate and avoidable duplication of effort if the agencies proceed with rail-specific regulation either before that mapping has been completed or while the process to produce it is still ongoing. Indeed, regulation has the real threat of stifling the innovation that is absolutely necessary in a constantly changing threat environment.

However, if TSA decides to take regulatory action, it must do so in a performance- and risk-based manner. The volume and detail of the questions posed in the ANPRM indicate consideration of prescriptive requirements. Yet, both DHS and TSA have expressed interest in

[3] *See* National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 2021), available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/; CISA, Cross-Sector Cybersecurity Performance Goals (Oct. 2022), available at: https://www.cisa.gov/cpg.

and commitment to being performance-based and data-driven.[4] The industry appreciates the efforts of TSA to promote performance-based and data-driven approaches in its SDs. However, when regulating the agency must go further to incorporate performance-based, not prescriptive, requirements. This is particularly important in cybersecurity, because of the fast-developing and evolving nature of cyber threats and the need to maintain flexibility and adaptability in risk mitigation and response capabilities. Prescriptive requirements can exacerbate cyber risk. Changes in tactics employed by malicious cyber actors will render the mandates of a prescriptive regulation obsolete. Innovation in cybersecurity can all too easily be undercut by the need to meet specific and detailed regulatory requirements and avoid the prospect of enforcement action. The undesired effect is solving for yesterday's attack rather than tomorrow's threat.

For any regulation, performance-based standards begin with a clear articulation of the problem to be solved. Without a clearly identified problem, it is impossible to know how the proposed policies or rules will resolve prevailing and emerging concerns, much less enable establishing a performance standard. Upon identification of the problem, TSA can then evaluate whether and to what extent existing performance standards applied by railroads, as well as other regulatory structures or requirements in effect or pending, address the cybersecurity concerns – with the least disruption to the parties' expectations and processes. To the extent other regulations cover the concerns, the agency should avoid duplicative requirements. For example, CISA has initiated the process, with a request for information to

[4] *See* ANPRM at 73531 ("In the year following issuance of the second pipeline SD, TSA determined that its prescriptive requirements limited the ability of owner/operators to adapt the requirements to their operational environment and apply innovative alternative measures and new capabilities.").

which railroads responded to in November 2022, to develop the statutorily mandated rulemaking to require reporting by critical infrastructure organizations of cybersecurity incidents not sooner than 72 hours after the affected entity reasonably believes a reportable event occurred.[5] TSA need not regulate here. However, if risk assessments have identified significant cybersecurity concerns or potential gaps, the agency could then pursue a balanced approach that leverages the strong partnerships maintained with railroads through well-developed coordination and information sharing structures; provides guidance on measures and actions to elevate cybersecurity posture for immediate mitigation of the significant cybersecurity concerns; and, where warranted, pursues narrowly tailored requirements aimed at long-term resolution in a risk-based manner. These are common principles of good governance.[6]

These points merit emphasis. Once a regulatory decision has been made to solve for a particular problem or fill a specific gap, the agency should do so in a narrowly tailored, performance- and risk-based manner where the benefits exceed the costs. AAR and ASLRRA appreciate that TSA is considering economic impacts, an area of particular concern for short lines, as evidenced by TSA's requests for cost numbers for a variety of the questions proposed

[5] *See* CISA, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, (Sept. 12, 2022) ("CISA RFI").

[6] *See* Exec. Order No. 12866 § 1(b)(1)–(2), 58 Fed. Reg. 51,735 (Sept. 30, 1993) ("[e]ach agency shall identify the problem that it intends to address (including, where applicable, the failures of private markets or public institutions that warrant new agency action) as well as assess the significance of that problem"; and "shall examine whether existing regulations (or other law) have created, or contributed to, the problem that a new regulation is intended to correct and whether those regulations (or other law) should be modified to achieve the intended goal of regulation more effectively.").

(e.g., B.4, C.1, C.5, C.6, D.5, D.7, E.1, F.1, G.1).[7] The agency also seems to recognize the value of performance-based rulemaking.[8] Many of the questions, however, imply a desire to define and require very specific actions of railroads (e.g., D.7, requiring third-party penetration testing; D.10 requiring monitoring and limiting access to OT and IT systems, D.12 requiring maintenance of certain security controls, D.14 requiring certain levels of architecture; E.2 requiring third-party certifier compliance assessments).[9] Such very specific actions should be avoided. Instead of requiring particular actions or technologies, TSA should identify the problem to be solved, in the context of prevailing and emerging cyber threats and significant security concerns. TSA then can set a performance-based standard for a railroad to meet in the most effective way its cybersecurity professionals determine based on risk assessments, network architecture and infrastructure, and critical functions.

In general, TSA has not identified a need for regulation of CRM, nor has it articulated any specific problem faced by the railroad industry, aside from general statements that rail may be vulnerable to cyber-attacks.[10] The mere possibility of a threat and lack of regulation in this particular space, on their own, do not provide a sound basis for regulating. The successful track record of the industry being proactive with regard to cybersecurity only highlights the concern with creating new regulations.

[7] *See* ANPRM at 73535-38. It should be noted that AAR and ASLRRA do not solicit specific costs from members for specific activities.

[8] *See id.* at 73534 ("To ensure that cybersecurity requirements sustain their effectiveness, regulations should provide for a continuous assessment of the current threat environment and ensure timely adaptation of dynamic security controls based on identified tactics, techniques, and procedures of malicious cyber actors and adversaries, while at the same time allowing for implementation of emerging technologies and capabilities that provide security controls that may be more relevant and effective for their intended purpose.").

[9] *See id.* at 73537-38.

[10] *See id.* at 73529.

As indicated earlier, working through RAN, for more than eight years railroads have consistently shared reports of significant cyber threats, incidents, and security concerns with a broad array of federal agencies and military components. Government intervention through regulation or directive did not produce this sustained effective practice. Rather, the industry acted innovatively, at its own initiative, to put into effect lessons learned from a joint government-industry tabletop exercise held for all modes by TSA in 2014. As a result, various federal agencies have received cybersecurity advisories and awareness messages based on reporting by railroads and industry organizations – including screen images whenever available – and recommendations provided on effective and sustainable protective and risk-mitigating measures. Again, these efforts were not driven by the compulsion of regulation, but business and operational necessity combined with dedication to the public-private partnership for cybersecurity. This fact is evidence there is no market failure here for which regulation is required.

Over the past year or longer, federal government assessments of a heightened cyber threat environment driven by escalated international tensions, including the Russian invasion of Ukraine, have reinforced the importance of sustained vigilance and timely reporting, along with information sharing by the government. Indeed, it may be more prudent for government to focus on sharing of intelligence related to threats and concerns, instead of identifying a list of steps that will be mandated for operators.

The railroad industry has repeatedly emphasized cyber vigilance in cybersecurity advisories disseminated widely to freight and passenger railroads, industry organizations, and suppliers. Under the requirements specified in TSA's first SD, railroads have continued to report suspect activity, network or system anomalies, and threats, incidents, and significant cybersecurity concerns in a timely and proactive manner – as they had done for more than eight years at their own initiative. This reporting has not indicated any recent increase in targeting of railroads generally, or of their critical operational or business functions specifically. Given this context, targeting of railroads may actually be less than other critical infrastructure sectors.

Indeed, other government components with cybersecurity responsibilities have not highlighted the railroad industry as particularly at risk. For example, CISA recently announced its "Planning Agenda" for the Joint Cyber Defense Collaborative ("JCDC").[11] The JCDC "gathers, analyzes, and shares information about cyber threats, providing real-world value and proactive solutions to defend today and prepare for tomorrow. JCDC is a leader in integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions."[12] The inaugural "Planning Agenda" notes efforts to address "risk topic areas" but cites only two critical infrastructure sectors – Energy and Water.[13] This is despite the determination by TSA that the railroad industry faced cyber threats of such magnitude as to necessitate exercise of emergency security directive authority.

[11] *See* Eric Goldstein, Exec. Asst. Dir. for Cybersecurity, "JCDC Focused on Persistent Collaboration and Staying Ahead of Cyber Risk in 2023" (Jan. 26, 2023), available at: https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023.

[12] CISA, JCDC FAQs, available at: https://www.cisa.gov/jcdc-faqs.

[13] CISA, JCDC 2023 Planning Agenda, available at: https://www.cisa.gov/2023-jcdc-planning-agenda.

Nor have any railroad representatives been appointed to the CISA Cybersecurity Advisory Committee ("CSAC"), an independent advisory body established in June 2021 that provides "independent, strategic, and actionable consensus recommendations to CISA on a range of cybersecurity issues, topics, and challenges, including, but not limited to: information exchange; *critical infrastructure; risk management*; and public and private partnerships."[14] When CSAC was established, the Colonial Pipeline incident had occurred just a few weeks earlier in May 2021 – with TSA issuing its first Security Directive on cybersecurity of pipelines before the end of that month. A joint industry group representing the aviation and surface transportation modes covered by TSA's Security Directives met virtually with CISA to seek appointment of members to CSAC. While there is an energy company member, there currently are no representatives from the aviation or rail industry.[15]

To be clear, by no means should these examples be viewed as critical of CISA's decisions regarding its JCDC plans, nor its appointment of such well-qualified advisory committee members. These initiatives are vital to leveraging the expertise and experience of government and industry. However, the lack of appointments and involvement of representatives of the railroad industry, and the failure to cite "Transportation" in the JCDC's 2023 Planning Agenda, does illustrate apparent substantial differences between TSA and CISA in assessments of the prevailing level of security risk and priorities for risk mitigation. At the very least, TSA should

[14] CISA, Cybersecurity Advisory Committee, Bylaws, available at: https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Advisory%20Committee%20Bylaws%20%287-8-21%29_508.pdf (emphasis added).

[15] *See* CISA, CSAC Members, available at: https://www.cisa.gov/csac-members (including a member from Southern Company which also owns pipelines); CISA, CSAC Charter, at 2-3, available at: https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Advisory%20Committee%20Charter_508%20Compliant.pdf (allowing up to three members from the Transportation Sector on the CSAC).

utilize a performance-based approach to the exercise of its regulatory authority, starting with a careful articulation the specific problem it is trying to solve with CRM regulations. Indeed, any stringent regulations with mandated prescriptive measures that inadvertently detract from long-standing, and proven, effective practices within the industry should be carefully considered and avoided, so as to not create unintended consequences.

As one example, the requirement in TSA's first SD to report cybersecurity incidents to CISA, led some railroads' cybersecurity leads to question their authority to share that information with other railroads and with organizations in other modes and critical infrastructure sectors. The perception is the first SD's requirement to report renders the information submitted to CISA subject solely to government action. An essential pillar on which the effectiveness of the rail industry cybersecurity program rests is proactive and timely sharing of information on confirmed or apparent malicious cyber activity. Early sharing of observed or experienced indicators, with recommended mitigation actions, informs vigilance widely, enables confirmation or refinement of protective measures, and narrows the potential for a successful disruptive attack. Hesitancy or failure in sharing information because of a perception that only the federal government is authorized to do so as a result of a directive or regulation undercuts effective cybersecurity practice in the industry – and potentially exacerbates risk. Again, this is just one example of how government action in the cybersecurity space can actually be disruptive to or distract from well-established cyber risk mitigation structures.

III. Regulations Must Recognize Differences in Pipelines and Railroads

It is clear that the ANPRM focuses on both pipelines and railroads because of the issuance for those industries of the similar SDs over the last two years.[16] As TSA experienced with the drafting of and feedback on the SDs, pipelines and railroads are different types of critical infrastructure with differing operations, infrastructure, and network architecture – and, therefore, different approaches, priorities, and needs for cybersecurity. Among the areas of significant differences are the scope and type of operational functions conducted through automated industrial control systems; networks, systems, equipment and capabilities that comprise "critical cyber systems" under the SDs; communications and data flows across networks; and industry-level organization, coordination, and information sharing procedures and practices for cybersecurity. Based on insights gained in eight technical consultations held with representatives of pipelines and their industry associations, TSA produced a substantially revised and refined second SD for that sector in July 2022. These requirements were reflected in the draft of the then planned second SD for railroads, provided for review and feedback in August 2022.

At the industry's request, two technical consultations were held in September 2022 – during which chief information security officers and cybersecurity leads for railroads and industry organizations detailed how requirements developed for pipelines were either inapplicable to or infeasible for rail carriers. To its credit, TSA made substantial changes to alleviate the cited discrepancies and concerns. In similar vein, TSA should take great caution

[16] *See* ANPRM at 73531.

applying the same requirements to these two very different industries. Just as the agency issued separate SDs for each industry, if it decides to issue regulations for the industries on CRM, they should also be separate and distinct.

In addition, as was experienced with the SD issuance for pipelines and railroads, the agency should incorporate a streamlined process for seeking waivers or proposing alternative compliance measures through compensating controls. Some aspects of the eventual proposed rule may not apply to all covered railroads, freight and passenger, so a waiver process where entities can show an alternative means to reach the same standard, or where a particular standard is simply inapplicable, should be adopted. This approach will encourage innovation while also providing options, when necessary, for covered carriers to which certain aspects of a proposed regulation may not apply.

IV. Regulations Should Be Harmonized With Other Agencies

If TSA pursues regulation on CRM, it should develop these and all cyber-related rules with other federal authorities, statutory obligations, and actions in mind, especially CISA and other security agencies. As noted, it is important to avoid duplication or conflicts – and thereby reduce regulatory burdens on railroads as they meet the vital role they play in supporting economic growth and opportunity nationally. Overlapping requirements can also cause confusion in the regulated community – accentuating the importance of clarity on what subject areas and responsibilities the planned rulemaking will cover and why. Interagency coordination to harmonize requirements under consideration is essential – before rulemaking processes commence.

For example, CISA's planned rulemaking to meet the requirements of the *Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")* should govern the incident reporting field fully.[17] CISA's regulations should thereby preclude duplicative or conflicting mandated reporting requirements by TSA or any other federal government agencies and preempt action in this sphere by state and local governments.[18] Indeed, once CISA's regulation is adopted, there should be no requirement from TSA with regard to reporting of incidents. If TSA nonetheless does act to require cybersecurity incident reporting, its mandated measures should absolutely be harmonized with CISA's statutory requirement. To the extent CRM is deemed appropriate for regulation, TSA may take the lead, but must ensure that initiatives by other federal agencies do not overlap or conflict with TSA's efforts. TSA should also take care to harmonize any regulations here with forthcoming CPGs for the Rail Sector, to reduce fragmentation in approaches and take advantage of validated effective practices.

Overall, federal regulation must support the ability of covered entities to focus on encouraging and sustaining innovation in developing cyber defenses, proactively investigating cyber activity of concern, determining its significance and implications, and taking effective actions to mitigate the risk of harm. TSA taking the initiative to ensure that federal agencies are

[17] *See* CISA RFI.

[18] Relevant as well is the ongoing rulemaking initiative by the Securities and Exchange Commission ("SEC") that would require covered corporations, including many railroads, to make a public report on a cybersecurity incident within five days of its occurrence. *See* Security and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Notice of Proposed Rulemaking (Mar. 23, 2022). The mandate to report publicly undercuts Congress' intent and CISA's objective with the regulation to be promulgated under CIRCIA – which is to provide information for CISA to analyze amongst reporting across all critical infrastructure sectors for indications of a developing threat or significant cybersecurity incident and share the insights gained through timely alerts and advisories to inform actions to reduce risk exposure. With CIRCIA, Congress has clearly indicated that CISA is the lead agency for reporting, analysis, and warning on cyber threats, incidents, and significant security concerns.

aware of its regulatory requirements and initiatives, reasonably respect applicable bounds, and avoid duplicative, overlapping, or conflicting mandates will provide such support.

V. Cybersecurity and Resiliency Must be a Partnership

The railroad industry and TSA have developed a positive working partnership over the course of the agency's existence. Acting on its responsibility as Sector Risk Management Agency for the Transportation Sector, TSA has worked cooperatively with the railroad industry to advance our shared goals in security, cyber and physical. TSA should maintain and continue this partnership – one to which the industry stands fully committed – but not through regulation. Instead, TSA can assure timely access to threat intelligence and related security information, classified and unclassified; maintain multiple means for effective sharing of threat intelligence and related security information, classified and unclassified; and ensure, along with its other federal partners, timely analyses of reporting by railroads and other Transportation Sector entities against information maintained on threats, incidents, significant security concerns, and suspicious activity across the critical infrastructure sectors.

TSA and federal agencies must work consistently with industry to provide actionable insight into cyber threats and vulnerabilities, and their consequences, identified through threat and risk assessments, compulsory and non-compulsory reporting, and other forms of intelligence collection and analysis. However, it remains unclear whether a dedicated process has been established by CISA, or between CISA and TSA, to ensure timely analysis of reporting by pipelines, air carriers, airports, rail transit systems, and railroads on cybersecurity incidents.[19] Statistics cited by TSA indicate that more than 1,000 reports have been made by entities covered by the TSA Security Directives to CISA. To date, no summary of the types of incidents reported or analyses for trends, patterns, or indicators of concern among what Transportation Sector entities are reporting has been produced and shared. Nor have any analyses been provided of commonalities between cybersecurity incidents reported in the Transportation Sector and those by entities in the other critical infrastructure sectors. Fully leveraging the available information on cyber threats and vulnerabilities, and on recommended measures and actions to narrow susceptibility and mitigate risk, is just as, if not more, important to overall cybersecurity of the industry than the planned rulemaking. So supported, industry will be better positioned to anticipate and manage cyber risks.

An essential element of an effective CRM strategy is the deterrent actions and measures internationally that only government can take. Success in mitigating the risk of terrorism and violent extremism required two complimentary approaches – measures to enhance security posture and practices and harden infrastructure domestically and intelligence and military actions internationally. Similar linkage for deterrence is essential in cybersecurity as well.

Finally, as part of the partnership, TSA must ensure the industry benefits from capabilities and opportunities managed by federal agencies to support the constant effort to identify, mitigate, and respond to cyber threats, incidents, and significant security concerns. Examples include: expanding security clearances for key personnel; expanding access to secure communications equipment (video and telephonic) to enable quick dissemination of classified information and remote participation in classified briefings; and restoring regular sharing of

[19] *See, infra,* at 26-27 (discussing non-compulsory programs within CISA and FBI to share information).

classified information with security leads at Canadian companies that maintain Canadian government clearances. These measures alone, without further regulation, will present immediate benefits to cyber risk management across the industry.

Specific Topics/Questions

“B. Identifying Current Baseline of Operational Resilience and Incident Response”[20]

Established in 1999, RISC supports cybersecurity industry-wide and provides a collaborative forum for assessments, information sharing, evaluation of threats and vulnerabilities, and exchange of effective practices to mitigate risk. RISC applies the NIST Cybersecurity Framework in biannual evaluations of industry cybersecurity posture, plans, and practices to assess effectiveness and identify concerns. To mitigate supply chain risk, RISC produced a compilation of effective practices to guide information technology procurements. Additionally, RISC has established a cybersecurity information sharing and coordination group with the industry’s principal suppliers. Railroads’ cybersecurity teams employ layered protective measures and capabilities, apply information on threats, incidents, and security concerns from a range of sources, maintain, exercise, and update thorough cyber incident response plans, and augment skills – through training and experience – to maintain effectiveness as the threat environment evolves.

As TSA knows, RAN partners with government entities to analyze and widely disseminate information on security threats, incidents, and significant concerns, cyber and physical. In addition, AAR, ASLRRA, and the industry also coordinate cross-sector and cross-

[20] ANPRM at 73535-36.

modally through the Transportation Sector Coordinating Council, representing each of the transportation modes; the Critical Infrastructure Cross-Sector Council, representing each of the critical infrastructure sectors and subsectors; and STSAC, TSA's principal advisory committee on security and emergency preparedness that AAR's Assistant Vice President for Security chairs, and on which ASLRRA's security lead sits as a member. The information gained from engagement and interaction through these forums, which focus on threats – assessed and experienced – incidents, and effective practices for risk mitigation, is applied proactively by the railroad industry to reduce its cyber risk profile. These efforts have been effective at mitigating cyber risk without government regulation.

As noted, railroads generally engage in a continuous improvement process by conducting periodic assessments of their cybersecurity risk and refining or augmenting plans, capabilities, practices, and coordination procedures to expand and enhance efforts to mitigate risks. Railroads have identified their critical functions and applied protective measures and actions – specifically, for those systems which, if compromised, would disrupt the ability of the railroad to function. Further, railroads continually evaluate their cybersecurity posture in the context of evolving threats, which is why RAN is so integral to collective effectiveness. Based on the insights gained from threat assessments and cybersecurity advisories informed by analyses of incidents, alerts from government organizations, and reporting by critical infrastructure entities, the industry highlights actions, measures, and other controls to mitigate the risk of disruption to rail operations and to sustain resiliency. Active monitoring of railroad operational technology assets is conducted and, where feasible, network segmentation is utilized as well, which reduces risk. CRM, therefore, is an ongoing process that may not easily be captured in a rulemaking proposal.

“C. Identifying How CRM Is Implemented”[21]

Managing cyber risk in the rail industry is a continual process of recognizing and responding to prevailing, evolving, and newly detected threats and indicators of compromise or cybersecurity concern. While specific plans, measures, and actions to address cyber risk are likely to vary among railroads, the industry collectively exercises capabilities to detect, prevent, and respond to cyber threats and incidents. This exercise program has been in effect since the development and implementation of the overarching industry security management plan in the weeks immediately following the terrorist attacks of September 11, 2001. The scope of this plan, and the capabilities for its effective and sustained implementation, have been refined, enhanced, and expanded over time. From its inception, coordination procedures and threat-based measures have focused on cyber and communications security. The most recent update to the plan, completed in 2020, broadened the content on cybersecurity measures based on escalating threat levels and incorporated the elements of railroads’ cybersecurity response plans by reference. Significantly, for more than 10 years, officials with CISA, TSA, FBI, FRA, DoD, and Transport Canada have participated in the industry’s annual security exercise – either as observers or direct participants. Lessons learned from the exercises are specified – with an outline of planned actions to address them. The result is a continuous process of review of plans, procedures, and measures for preparedness and risk mitigation – both at industry level

[21] *Id.* at 73536.

and within individual railroads – driven by the shared experience and expertise of those involved in industry and government.

With regard to cybersecurity personnel, railroads designated cybersecurity coordinators and alternates years before TSA's issuance of the first SD in December 2021. Railroads also maintain dedicated cybersecurity staffs, whether in-house or through contracted services. The numbers of personnel assigned to these responsibilities vary based on size and scope of operations and risk profile of the railroad. As an effective practice, railroads provide for continuing professional education of members of their cybersecurity teams – including participation in training programs offered by federal government entities, notably, the Idaho National Laboratory, which provides invaluable experience through hands-on scenarios of both network defense and "red-teaming" as attackers seeking to perpetrate breaches and compromises.

A key element of support needed from TSA is obtaining security clearances in a timely manner to ensure access to actionable cyber threat intelligence and related cybersecurity information at classified levels. In similar vein, timely sharing of classified information depends upon options for secure communications. Challenges have persisted in connecting government agencies and railroads through the disparate secure video-teleconferencing networks maintained by federal government organizations. A necessary initiative is identifying, testing, and repeatedly exercising the SVTC connections that work most effectively for railroads subject to TSA's SDs. Additionally, broader access to secure telephone equipment enables timely warning in the event of a specific threat or incident to specific railroads or the industry as a whole. While the video element is lacking, secure telephone equipment does enable participation in SVTC calls. Again, broader deployment of this equipment is essential. To TSA's credit, it has approved 13 railroads and industry organizations for new deployments that will happen in the near term. Longer term, secure phones should be available for the appointed Cybersecurity Coordinators and Rail Security Coordinators appointed to meet TSA requirements set by security directive or regulation. The shared objective for industry and government is to assure timely leveraging of threat intelligence and security information for prevention and risk mitigation.

For short lines implementing new or revised CRM programs in response to the current SDs, or under future regulations, there is an expectation that additional in-house expertise will have to be hired or developed, or additional third-party support will be required. These costs will vary among short lines. In some cases, costs could prove to be significant, further highlighting the need for CRM requirements to be implemented on performance-based principles that allow small organizations to tailor their CRM programs and costs to their risk and the relative impact of a cyber incident on their railroad on the national freight network as a whole.

"D. Maximizing the Ability for Owner/ Operators To Meet Evolving Threats and Technologies"[22]

In response to whether railroads should be required to restore or recover compromised information stolen from their networks within a defined timeframe, AAR and ASLRRA do not believe that timing mandates related to restoration and recovery should be imposed on the industry. The business necessity of prompt and effective action to preserve or resume normal

[22] *Id.* at 73536-38.

operations is the essential incentive. No rail operator wants to unnecessarily delay recovery or restoration of systems or data. Regulatory compulsion with mandated timelines is wholly unnecessary. Deterring and pursuing malicious cyber actors is an appropriate, and essential, role for the responsible federal government departments and agencies. TSA can provide an invaluable service by working in concert with its counterparts to ensure malicious actors are identified, investigated, and pursued – and their sources of support deterred, constrained, or eliminated.

Furthermore, mandating timeframes for response and recovery actions does not accord with performance-based rulemaking. No two incidents are the same. There are occasions – frequently – when the data is simply not retrievable. The complexity and severity of any particular incident will dictate the best means and projected timeframe for recovery. A regulatory timeline might force entities to focus on recovery speed at the expense of immediate and long-term effectiveness and sustainability. Compelling covered entities to pursue efforts to recover stolen data may prompt actions that federal cybersecurity agencies and components urge against simply to avoid civil fines or penalties for violation of a regulation (e.g., acquiescence to demands for ransom payments). Organizations that have suffered a cyber-attack disruptive to operations will strive to restore compromised data and critical functions as expeditiously as practicable – in accordance with processes, procedures, and actions outlined in their cyber incident response plans ("IRP").

As to the industry's critical cyber systems, if TSA considers rulemaking on this subject, the term should not be defined based on specific "systems." Given the diversity and complexity of operators' networks, it would not be prudent for the government to attempt to define what "systems" are in scope. Instead, it is more appropriate, and effective, to focus on critical functions – that is, those capabilities necessary for the railroad to safely assemble and move trains that transport freight and passengers. Any future regulation should not specify systems and applications or mandate measures or actions for their protection from cyber threats. Rather, applying a performance-based approach, railroads should be accorded the flexibility – based on their risk assessments – to define their critical functions, determine what systems are in and out of scope, and identify the most effective and sustainable measures employed for cyber risk mitigation.

With regard to technology and emerging threats, the federal government can play an important and continuing role in helping to keep industry apprised of advanced capabilities, and their purposes and utilization, for cybersecurity. However, under no circumstances should a TSA regulation mandate adoption of a particular technology. Inherent in performance-based rulemaking is affording industry the ability to innovate and adopt effective and sustainable technological solutions for enhanced cybersecurity posture. This form of continuous evaluation and enhancement is accomplished far more nimbly by the private sector based on risk assessments and identified priorities for mitigation. At the same time, if government is aware of emerging technologies that could aid industry entities in reducing cyber risks, it should inform them through a consistent, well understood, and regularly utilized information-sharing process.

Similarly, a key element in TSA's role, with its federal government partners and international partners in Canada and Mexico, should be to ensure awareness across transportation modes of emerging threats and cyber-attack tactics, techniques, and procedures experienced across government and other critical infrastructure sectors. This action alone, consistently pursued in a timely manner through focused alerts and advisories, can contribute substantially to cyber risk mitigation. Federal agencies can advise of such threats, but it becomes more complicated if the government requires specific action in response. The railroad industry already has every incentive to mitigate and effectively manage its risk.

Key support already comes from non-compulsory federal cybersecurity information sharing programs. CISA's Shields Up campaign is an excellent example of the public-private partnership in action – without regulatory compulsion. Through Shields Up, CISA identifies and describes threats and vulnerabilities for the critical infrastructure community. Alerts and advisories relate the tactics employed by malicious cyber actors, vulnerabilities they exploit, indicators of compromise or concern with technical details, and recommended actions and measures to narrow susceptibility and mitigate risk. This information narrows the potential for cyber-attacks to expand and cause disruptive impacts across sectors and industries. Recommended protective measures and actions, including instructions on security patching of identified vulnerabilities, support resiliency – in the near and long terms. The FBI provides a similar caliber of support through its Cybersecurity and Private Sector Divisions. FBI Private Industry Notifications ("PINs"), apply insights gained in criminal investigations and intelligence analyses of cyber-attacks and attempts – focused on tactics employed, vulnerabilities exploited, indicators of compromise and concern, and recommendations for effective and sustainable protective measures and actions.

The industry's RAN leverages the products of these exceptional programs through cybersecurity advisories and awareness messages that inform vigilance and drive protective actions for freight and passenger railroads. It may be that some of the alerts and advisories produced by CISA, or the PINs produced by the FBI, are based on reporting by Transportation Sector organizations. But any such linkage is not made clear to industry stakeholders in the transportation modes. This gap is significant. The incentive to report in a timely and thorough manner results not from the compulsion of regulation, but from demonstrated value – that reports are analyzed and applied in timely and constructive ways to inform measures and actions to enhance cybersecurity posture and mitigate risk. TSA can provide an invaluable service by highlighting whether and how reporting by Transportation Sector organizations has contributed to, or implicates, evaluation of the cybersecurity concerns and recommended mitigation measures addressed in the awareness materials produced by CISA or FBI. Ultimately, whether a regulation on CRM is promulgated or not, no action by any federal agency should detract from the work performed through such non-compulsory programs that inform proactive measures to reduce cyber risk.

Similarly, TSA must avoid requiring specific actions, like third-party penetration testing. While recommending such testing of resiliency might be appropriate, requiring it, or any other specific mitigation action, is not performance-based. Many critical infrastructure organizations, including railroads, already conduct penetration testing, as it can be a key part of a robust CRM program. But it can impose risks and is usually deployed with care to certain systems or operations as part of an overall program. Each operator should remain free to determine if, when, and how to use penetration testing in their CRM programs, and to define the parameters of it. Further, it is not difficult to envision some superior or alternative testing protocol or procedure being developed in the future. Were penetration testing as currently understood and applied to be required by regulation, railroads would be locked into a practice that may not be as effective as advanced alternatives. Finally, a requirement for third-party testing could prove onerous for short lines, many of whose performance-based assessments of cyber risk may not justify the cost. TSA must therefore only design risk-based standards that could be met in varied ways by railroads and other covered transportation organizations based on their assessments of cybersecurity risk.

As with testing, TSA must not dictate through regulatory requirements the duration or caliber of experience that railroads' cybersecurity employees must possess. Railroads are best positioned to determine the needed skills, experience, initiative, and potential in recruiting members of their respective cybersecurity teams, and any third-party support they may require. Flexibility is particularly appropriate for cyber expertise in rail workforces, given the widely-recognized national shortage of skilled and experienced talent in this field across the private sector and government.[23] As noted earlier, TSA should focus its efforts on assisting railroads in maximizing the capabilities of their cybersecurity workforce by supporting applications for and issuance of security clearances – to ensure awareness of the scope and nature of threats, vulnerabilities, and security concerns. This investment will produce dividends in more thorough and effective reporting and in innovative efforts that will assure a sustained,

[23] Presidential Executive Order 13870, America's Cybersecurity Workforce (May 2, 2019) found that "[t]he Nation is experiencing a shortage of cybersecurity talent and capability" and NIST recently estimated that the shortage of cybersecurity professionals is estimated to be 2.72 million, https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf while others put the shortfall higher. This shortfall is affecting federal agencies and private companies, and may limit operators' ability to meet specific government mandates about workforce expertise.

and continuously reviewed and improved, cybersecurity posture to meet prevailing and emerging cyber threats.

“E. Identifying Opportunities for Third-Party Experts To Support Compliance”[24]

With regard to third parties, the government should not require their utilization. Again, this level of detail in a regulatory mandate is simply not performance-based rulemaking. Allowing for the utilization of third parties to meet cyber risk mitigation priorities and objectives is important – especially for those entities that do not have in-house expertise. So, it is important that there not be any prohibition or limitation placed on utilization of third parties. Nor, however, should retention and utilization of third parties be required.

As a prudent practice, entities that utilize third parties typically vet their expertise, credentials, experience, and references – as they have done regularly in contracting for security services based on integrity and trust. It is unclear how TSA would be able to enforce any requirements for third parties, given that the agency’s jurisdiction and authority are limited to transportation organizations. As such, TSA should allow for self-certification, which is a common practice in the transportation safety community. Be it aviation, automobile manufacturers, or rail safety, the government allows industry to self-certify to the government standard. Enforcement is conducted against that self-certification. The reasoning is that the regulated entity has all the incentive necessary to ensure compliance with the safety standards. It is no different in the cybersecurity context.

[24] ANPRM at 73538.

Finally, TSA may need to consider carefully how third parties will be affected by any rules. Short lines are particularly dependent on third-party suppliers for the design and operation of many of their technology systems, including many of those maintained internally by Class I railroads. Some rail operators may not have full visibility into the security operations of diverse suppliers, but it is important that suppliers are considered as part of overall CRM. TSA may want to consider how to engage with critical rail suppliers to discuss best practices and the relevance of past government guidance on risks facing managed service providers and others in the delivery of services to rail operators. If regulation of some suppliers happens through the appropriate Sector Risk Management Agencies, TSA should consider impacts of such actions on its regulated entities.

A critical area meriting expedited action is the establishment of standards or effective practices for production by vendors of software bills of materials ("SBOM"), which is "a key building block in software security and software supply chain risk management. An SBOM is a nested inventory, a list of ingredients that make up software components."[25] This information substantially aids and supports critical infrastructure owners and operators to determine whether identified vulnerabilities apply to software products used in their networks, systems, and assets; and to guide actions to resolve them through security patches and other mechanisms. Unfortunately, this essential resource remains largely unavailable to railroads and other critical infrastructure owners and operators – even with the prevailing assessments of a heightened cyber threat environment during the past year-plus. As CISA notes, "SBOM work has advanced since 2018 as a collaborative community effort, driven by National

[25] CISA, Software Bill of Materials, available at: https://www.cisa.gov/sbom.

Telecommunications and Information Administration's (NTIA) multistakeholder process."[26] The railroad industry supports this initiative. But it is now entering its fifth year. With the issuance of the SDs, TSA has taken the position that "business as usual" does not pertain for cybersecurity in the covered transportation modes. A similar impetus must be applied to drive completion by CISA of the SBOM initiative – especially for networks, systems, and devices used in the Transportation Sector for critical functions.

"F. Cybersecurity Maturity Considerations"[27]

If TSA makes the determination to regulate further in the cyber risk space, the rules developed should loosely reflect the types of requirements, revised for a more performance- and risk-based approach, specified in the SDs. This approach would produce the lowest impact to the regulated entities from a cost, resource, and operations perspective, while acknowledging the extensive efforts on tight timelines dedicated to compliance with the provisions of the directives. Often government regulators properly distinguish between Class I and short line railroads in establishing regulatory requirements. In this case, however, due to the interconnectedness of our physical rail networks, and in some instances computer networks, AAR and ASLRRA urge TSA to maintain similar risk-based approaches for all rail operators. The industry has cooperated to protect our networks to date and needs the freedom to do so in the future.

[26] *Id.*

[27] ANPRM at 73538.

In addition, though, a planned rulemaking should allow for an efficient waiver process, and clear demarcation of which railroads, by name or other characterization, are included in the scope of a future regulation. This is especially critical for smaller entities that lack the infrastructure or risk profile to merit imposition of compulsory measures or actions. Finally in this regard, a regulation on CRM must incentivize covered railroads and other transportation entities to act innovatively and flexibly on the results of cyber risk assessments.

As noted, harmonization by TSA with other federal requirements is integral to the public-private partnership and success of any CRM strategy. To the extent there is conflict, duplication, or overlap with existing or planned mandates, TSA should work through interagency coordination to reduce burdens on the industry by harmonization. On cyber incident reporting, federal statute directs CISA to promulgate a regulation that requires critical infrastructure organizations to report covered cybersecurity incidents not sooner than 72 hours from identification. This clear demonstration of Congressional intent merits universal application and respect. The same period should pertain for reporting under TSA's first SD – not the 24-hour period mandated. When the CISA rule is promulgated, it should be the only federal requirement on cybersecurity incident reporting. Similarly, any regulation developed following this ANPRM should be the only governmental requirement for CRM applicable to railroads.

“G. Incentivizing Cybersecurity Adoption and Compliance”[28]

The railroad industry launched coordinated and unified efforts to manage cyber risk over two decades ago. The commitment has never abated. The scope of participation in the industry’s RISC has expanded. Recurring assessments and exercises have identified risk-based priorities for enhancements in capabilities, coordination procedures, and protective measures and actions. Continuous, and consistent, sharing of information on cyber threats, incidents, and significant security concerns has informed vigilance and enabled measures and capabilities for effective prevention and response – in support of resiliency in operations.

Insurance against cyber incidents, while increasingly more common across critical infrastructure sectors and industries, should not be mandated by federal regulation. Divorced from determinations based on cybersecurity risk assessments, this type of requirement will escalate costs on industry. Already, as the markets change, cybersecurity insurance premiums are becoming more expensive – with even less value to the customer given changing rules on what is and is not covered. This trend will be exacerbated if a federal regulation requires railroads and other transportation organizations to procure insurance on specified parameters. The government should not regulatorily subsidize the insurance industry by requiring certain sectors of the economy to purchase insurance.

In closing, and in response to the tools that TSA can provide, it is absolutely imperative that the agency operate as a true partner with industry. TSA’s work to increase and improve outreach to industry during the process of drafting and implementing the SDs should continue to be built upon, particularly with regard to short lines that they are newly engaging with on

[28] *Id.* at 73538.

cyber security issues. TSA, with other federal agencies, should work to provide as much feedback on cyber incident reporting as possible. Actionable information, shared in a timely and effective manner, contributes substantially to cyber risk mitigation and, thereby, supports operational resiliency.

Conclusion

AAR and ASLRRA appreciate TSA's focus on managing cyber risks and believe TSA should clearly articulate any problem with cyber risk it believes exists prior to resorting to regulation. Regulation should not be a forgone conclusion. AAR and ASLRRA look forward to continuing to collaborate constructively with TSA as it proceeds in this docket.

Respectfully submitted,

Kathryn D. Kirmayer
J. Frederick Miller Jr. (*admitted in MD*)
Association of American Railroads
425 Third Street, SW
Washington, D.C. 20024
(202) 639-2100

Counsel for the Association of American Railroads

Sarah Yurasko

Sarah G. Yurasko
American Short Line and Regional Railroad Association
50 F Street NW, Suite 500
Washington, DC 20001
(202) 585-3448

Counsel for the American Short Line and Regional Railroad Association

February 1, 2023