BEFORE THE
DEPARTMENT OF HOMELAND SECURITY,
TRANSPORTATION SECURITY ADMINISTRATION

NOTICE OF PROPOSED RULEMAKING –
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") (collectively, the "Associations") respectfully submit these comments in response to the Notice of Proposed Rulemaking ("NPRM") on Enhancing Surface Cyber Risk Management, issued by the Transportation Security Administration ("TSA") on November 7, 2024.[1] While surely well-intentioned, the proposed rule is often too focused on matters that do not meaningfully contribute to a robust cybersecurity program; regulation of these areas would place unnecessary demands on railroad operations and create needless expenses—sometimes with the unintended consequence of distracting and detracting from railroads' existing security efforts.

BACKGROUND

AAR's freight railroad members include the six Class I railroads, as well as scores of U.S. short line and regional railroads. Together, they account for the vast majority of freight railroad mileage, employees, and traffic in the United States. With their Canadian and Mexican 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

[1] Enhancing Surface Cyber Risk Management, 89 Fed. Reg. 88,488 (Nov. 7. 2024).

members, which include Amtrak and various commuter railroads, account for more than 80 percent of passenger railroad trips in the United States.

ASLRRA represents over 600 small business short line and regional railroads throughout the United States, along with hundreds of vendors providing products and services to those railroads. ASLRRA's members operate 50,000 miles of track or nearly 30 percent of the national railroad network, providing the first- and last-mile connection between farmers and manufacturers and consumers. ASLRRA's members include Class II and Class III railroads, which are defined as railroads earning annual operating revenues between $47.3 million and $1.05 billion and $47.3 million or less, respectively.

These diverse association members have been at the forefront of cybersecurity in the transportation sector since the turn of the century. For example, the Rail Information Security Committee ("RISC"), an industry-formed and -led coordination group established in 1999, is a key part of the rail industry's unified, cooperative cybersecurity efforts as they exist today. RISC is comprised of railroad chief information security officers and information assurance officials, as well as industry organizations, and augmented by AAR and ASLRRA security staff. Collectively, these industry experts share information on significant cyber threats, incidents, and indicators of cybersecurity concern; establish best practices for effective risk mitigation to inform vigilance; and elevate security posture, industry wide. Thus, the rail industry has embraced cybersecurity risk management for more than 25 years and is willing and able to work cooperatively on industry safety initiatives.

However, even the industry's best efforts can be frustrated by unclear, unnecessarily prescriptive, or conflicting regulations. The proposed rule takes a one-size-fits-all approach that, at times, ignores the realities of modern railroading, as well as the needs of small railroads. Accordingly, these comments address the concerns of the Associations and their members—which include unclear or overly burdensome proposals as to governance, "critical cyber systems," and supply chain management, as well as cybersecurity incident reporting requirements that are inconsistent with already existing regulations—and suggest various ways in which TSA might improve upon the rule in furtherance of the shared goal of enhancing cybersecurity.

COMMENTS

The Associations and their members have a number of concerns with the proposed requirements contained in the NPRM. Chief among these are the governance provisions, including but not limited to the requirement that the primary Cybersecurity Coordinator be a U.S. citizen; the inclusion of Positive Train Control ("PTC") as a "Critical Cyber System" without a risk-based justification; the proposed enforcement—*by the railroads*—of various supply chain requirements; the lack of regulatory harmonization between government entities (even those under the umbrella of DHS) with respect to the reporting of cybersecurity incidents; and, finally, the applicability of the proposed rule to Class II and III railroads, which, if interpreted expansively, would include many more railroads than TSA likely intends.

I. Governance

As per the NPRM, owner/operators would be required to annually conduct a Cybersecurity Assessment Plan ("CAP"), an enterprise-wide cybersecurity evaluation that would identify the current profile of cybersecurity (including physical and logical/virtual controls) compared to the target profile.[2] Following the CAP, railroads would be required to develop a Cybersecurity Operational Implementation Plan ("COIP").[3] Several requirements of the COIP, as presently proposed, contain overly burdensome—and, sometimes, outright impossible—requirements, many of which would not meaningfully contribute to improving cybersecurity. Particularly problematic areas include governance provisions that would require the identification of named individuals responsible for the governance of the owner/operator's Cybersecurity Risk Management ("CRM") Program, including multiple Cybersecurity Coordinators, who are to be available ***at all times***, irrespective of a railroad's hours of operation or the presence of an actual cyber threat, plus an "accountable executive," distinct from the Cybersecurity Coordinators, who functions at "a level between the most senior-executive leadership and the implementation/operations level of the organization."[4]

---

[2] Id. at 88,491. The requirements of the CAP are unclear. This is discussed more fully below, in Section VI.C.

[3] Id.

[4] Id. at 88,515. Submission methods for the COIP need to be clarified. As discussed below in Section VI.D., the COIP, as well as any other security-related documents, ***must*** be maintained at the railroads and reviewed by TSA through on-site visits.

A. Cybersecurity Coordinator(s).

The proposed rule would codify the requirement that a covered owner/operators designate a "primary Cybersecurity Coordinator" who is "a U.S. citizen . . . eligible to receive a security clearance."[5] In addition to this primary Cybersecurity Coordinator, owner/operators must "identify . . . ***at least one*** alternate Cybersecurity Coordinator" at the headquarters level.[6] Per the NPRM, these Cybersecurity Coordinators would be required to be "accessible to TSA 24 hours per day, seven days per week."[7]

These proposed requirements exemplify the problems with the government's one-size-fits-all approach. For example, the interconnected railway network spans from Canada to Mexico, and the designation of a U.S. citizen as primary Cybersecurity Coordinator creates significant problems for the Canadian-based railroads, whose headquarters are largely staffed by Canadian citizens. Under earlier TSA security directives, the citizenship requirement sometimes necessitated unreasonable "work arounds" by the Canadian railroads.

Furthermore, there is no security justification for such a stringent requirement. The United States and Canada share intelligence information as part of the Five Eyes intelligence alliance. This requirement should be stricken, or a waiver program established.

---

5 Id.

6 Id. (emphasis added).

7 Id.

In addition, the proposed mandate for one or more headquarters-level alternates to serve as backup to a primary Cybersecurity Coordinator ignores the fact that short line railroads are small businesses, with limited resources. Indeed, many do not operate every day, with some smaller operations running as infrequently as one day a week. The need for additional personnel could cripple smaller railroads and would force larger operations to bear the unnecessary expense of redundant staff.

Moreover, it is simply not feasible to expect one person—or even two people—to be available to TSA 24 hours per day, seven days a week. Basing the exchange of potentially critical security information on the availability of two identified individuals, rather than allowing railroads to identify the most efficient means of sending and receiving such information, would do railroads of all sizes a disservice; Class II and III railroads would be required to have staff available at times that are unrelated to the operations of their railroads, while Class I railroads would be prevented from utilizing their larger security and IT operations to insure that information is ingested or shared in the most efficient manner. TSA itself does not have a designee (or designees) available for the Associations or their members to contact 24 hours per day, seven days a week. The government must recognize that this is an unrealistic requirement, and limit expectations of availability to times when there is an identified risk.

Instead of being overly prescriptive in how private businesses approach their hiring or how they meet their responsibilities under the proposed rule, TSA must focus on its desired outcome; here, the NPRM notes that TSA's goal is "a contact in a position to understand cybersecurity problems; immediately raise issues with, or transmit

information to, . . . appropriate corporate or system leadership; and recognize when emergency response action is appropriate."[8] How those requirements are met should left to the discretion of the owner/operator. Doing so would achieve the stated goal of the TSA to be performance-based in its rulemaking, rather than prescriptive.[9]

B. Accountable Executive.

In addition to multiple Cybersecurity Coordinators, the NPRM proposes that organizations identify a named individual ''as responsible and accountable for planning, resourcing, and execution of cybersecurity activities."[10] This "accountable executive" would be tasked with "activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning."[11] The NPRM further notes that the accountable executive "should ***not*** be the Cybersecurity Coordinator or otherwise have responsibility for day-to-day management of the IT or OT system" and "should function at a level between the most senior-executive leadership and the implementation/operations level of the organization."[12]

Mandating the governance and leadership responsibilities of employees within the private sector constitutes government overreach and is unnecessary for cybersecurity purposes—particularly when prohibited employees are well suited to perform the required

---

8 Id.

9 See id. at 88,499 ("TSA is proposing a performance-based regulation for cybersecurity. . . .").

10 Id. at 88,514.

11 Id.

12 Id. at 88,514-15 (emphasis added).

functions. Again, such a requirement is prescriptive, not performance based. It would be sufficient for the stated goals of the NPRM that a qualified individual fulfills the duties of the accountable executive, as outlined in the NPRM, ***without*** a mandate as to the individual's other responsibilities or level within an organization. Moreover, such a proposal is all but impossible for smaller railroads, where the CEO is the only person overseeing the individual at the IT/OT implementation/operations level of the organization, and the hiring of additional personnel would be crippling. Accordingly, the requirement for an additional accountable executive, who is distinct from the Cybersecurity Coordinator, should be removed from the final rule.

II. Critical Cyber Systems

As proposed, the methodology for identification of critical cyber systems would encompass virtually every component of a train. The proposed methodology requires owner/operators to "identify Information Technology and Operational Technology systems that ***could be*** vulnerable to a cybersecurity incident."[13] The NPRM goes on to state that owners/operators must include information "regarding the ***likelihood*** of the system being subject to a cybersecurity incident."[14] The ability of railroads to identify which of its cyber systems are truly critical, such that their unavailability would have serious operational impacts, and to focus on those systems is imperative.[15] Without a limiting factor based on

[13] Id. at 88,563 (emphasis added).

[14] Id. (emphasis added).

[15] This is especially true for Class II and Class III railroads, which need to effectively and efficiently allocate scarce resources.

a system's ***actual*** impact on railroad operations, the identification requirements become overly inclusive and unduly burdensome to implement.[16]

Particularly concerning is the inclusion of Positive Train Control ("PTC") as a critical cyber system. This is a prescriptive requirement with little security justification.[17] PTC is a set of technologies that prevent the most serious human-error accidents like train-to-train collisions and over-speed derailments. There are three main elements of a PTC system, which are integrated by a wireless communications system: (1) the onboard locomotive system, which monitors the train's position and speed and activates braking as necessary to enforce speed restrictions and unauthorized train movement; (2) the wayside system—which includes multiple components as diverse as radio towers and wayside interface units—handles communications between the "right of way" and the back office; and (3) the back office server, which acts as a storehouse for information related to the rail network and transmits the authorization for individual trains to access new segments of track.

Fundamentally, PTC is ***safety*** technology; it is not ***operational*** technology. Trains are capable of operating without PTC; indeed, PTC was designed as an overlay system implemented in addition to operational rules. As such, there is no risk-based justification for the inclusion of PTC as a "Critical Cyber System."

---

[16] The burdens of the proposed language are only further exacerbated by the requirement that "owner/operators should also consider programmable electronic devices, computers, or other automated systems which are used in providing transportation; alarms, cameras, and other protection systems; and communication systems, and utilities needed for security purposes, including dispatching systems." Id. The rule would be all-encompassing, without regard for what is ***actually*** necessary for train operations.

[17] A singular footnote concerning an outage is used to justify this highly burdensome expense, as explained more below. *See* id. at 88,517, n.161.

Moreover, the proposed language is unclear as to what components of PTC are intended to be covered. While no component of PTC is necessary for train operations, the final rule's inclusion of wayside systems would be especially burdensome. Indeed, AAR estimates that it could cost railroads nearly $17,000 ***per* wayside** in order to implement the proposed rule. AAR further estimates that Class I railroads operate more than 15,000 radio towers and more than 30,000 wayside interface units, with more coming online in the next five years. This means that a conservative estimate of including ***even a singular component of PTC*** under the final rule could cost the industry hundreds of millions of dollars to implement, with additional expenses for annual maintenance. As such, the Associations believe that TSA has significantly underestimated the costs associated with the proposed rule's new requirements.[18]

The inclusion of PTC as a critical cyber system in the final rule would create burdens for the railroads that are simply unsustainable, without adding to cybersecurity in any meaningful way. Indeed, diversion of railroads' limited resources to an excessive mandate will undermine ***actual*** risk-based network protection priorities. As such, the final rule must clarify remove PTC as a "critical cyber system" and permit railroads to determine what truly constitutes an operational risk in the event of a cybersecurity incident.

III. Supply Chain Risk Management

The NPRM proposes new requirements for supply chain risk management, including a mandate that railroads ensure that any new software purchased for, or to be installed on, critical cyber systems meets the Secure-by-Design and Secure-by-Default principles

[18] The estimated 10-year cost of the proposed rule is $2.6 billion. See id. at 88,532.

promulgated by the Cybersecurity & Infrastructure Security Agency ("CISA").[19] Notably, however, it would be left to the railroads to enforce these requirements. This rule is simply unenforceable without the government's assistance to hold suppliers accountable, and TSA cannot expect owner/operators to impose and administer rules that TSA itself does not have the authority to enforce.

In addition, the proposed rule has the potential for several unintended consequences. Among these, the rule could reduce vendors' willingness to work with the railroads. This could reduce competition between vendors (which are already limited in number), leading to skyrocketing costs, reductions in innovation, and unnecessary restraints on railroad growth.

Moreover, the proposed rule is simply not reflective of actual business practices. Owner/operators have preexisting contracts with their vendors—some of which cover significant periods of time—and must comply with the terms contained therein or potentially face steep consequences. Railroads also need the flexibility to run their operations as they know best. As such, the final rule must eliminate this provision.

IV. Cybersecurity Incidents

Multiple federal agencies impose cybersecurity reporting requirements on the transportation sector, including TSA, the Federal Railroad Administration ("FRA"), the Environmental Protection Agency ("EPA"), the Department of Transportation ("DOT"), the Department of Defense ("DOD"), and, for some railroads, the Securities and Exchange Commission ("SEC"). The TSA alone "has eight requirements applicable to aviation and

[19] See id. at 88,518.

surface transportation," including passenger railroad carriers, rail transit systems, and freight railroad carriers.[20] Many of these regulations and laws conflict with one another, creating a hodgepodge of fragmented and competing rules with which railroads must comply. In this way, TSA's proposed rule is no different, but there is opportunity to harmonize the requirements of TSA's forthcoming rule with another reporting requirement to CISA under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[21]

Per the NPRM and the security directives before it, TSA now proposes to require the reporting of a cybersecurity incident ***to CISA***, including incidents "under investigation," within just 24 hours of identification—a burdensome requirement that would detract resources from responding to an attack, and conflicts with the period mandated by Congress under CIRCIA.[22] CIRCIA amends the Homeland Security Act of 2022 to require *CISA*—***not TSA***—to promulgate a regulation requiring reporting of covered cyber incidents to the agency "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred."[23] With CIRCIA, Congress mandated that CISA regulate the reporting of "covered cyber incidents," demonstrating the intent that CISA

---

[20] See DHS, Office of Strategy, Policy, and Plans, *Harmonization of Cyber Incident Reporting to the Federal Government Report* 10 (Sep. 19, 2023) ("*Harmonization Report*").

[21] See Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") Reporting Requirements, 6 CFR Part 226.

[22] 89 Fed. Reg. at 88,522.

[23] Pub. L. No. 117-103, 136 Stat. 49, at 1043.

serve as the lead federal agency, not TSA.[24] Therefore, for covered entities, CISA's requirements must supersede TSA's cybersecurity incident reporting. TSA's reporting requirement should be removed or revised to align with CIRCIA, and TSA should coordinate with CISA as their statutorily mandated rule is finalized. Given the clear expression of Congressional intent with CIRCIA, the period of 24 hours set by TSA in the proposed rule for reporting ***to CISA*** should be eliminated or, at least, it should be revised to harmonize with the 72-hour standard under section 2242(a)(1)(A) of CIRCIA.

Moreover, TSA's proposed definition of reportable incidents is much broader than CIRCIA's statutory requirements and does not have a severity of impact threshold. Given CISA is the government's congressionally mandated lead for incident reporting, the TSA should either eliminate its reporting requirement or harmonize its rule with CISA's. Indeed, "unauthorized access" is defined to include a "non-malicious policy violation."[25] A mere policy violation simply does not constitute a cybersecurity incident of the nature that would impact train operations.[26] These conflicting definitions and time frames for incident reporting must be eliminated from the rule entirely, given CISA's role, or be harmonized to provide consistency for owner/operators, and an impact threshold related to the continuous operation of trains must be added to the final rule.

---

[24] Pub. L. No. 117-103, 136 Stat. 49, at 1038, 1040-1042 (establishing CISA as the government entity to, among other things, "receive, aggregate, analyze, and secure" reported cyber incidents, and to "coordinate and share information with appropriate Federal departments and agencies").

[25] 89 Fed. Reg. at 88,507.

[26] TSA's proposed reporting requirements are broader and lower than the government imposes *on itself,* as federal guidelines state that federal departments and agencies are expected to report to CISA those cybersecurity incidents "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence."

V. Overinclusion of Class II and Class II Railroads

Although the proposed rule includes language that would exclude the majority of Class II and III railroads from many of the cyber risk management requirements, several provisions have the potential to needlessly envelop railroads with operations that do not represent a security risk to their localities or the national network. For example, the NPRM proposes to include all Class II and III railroads with annual operations in excess of 400,000 train miles.[27] This provision is based on an incorrect assumption that these railroads operate on such a scale that an operational interruption would significantly impact the flow of freight across the national network. To put things in perspective, however, Conrail, which is the largest of these Class II and III operations, operated approximately 2.77 million train miles in 2023; this is only 14% of the total train miles operated by the smallest Class I railroad in the same year.[28] At the 400,000 train mile threshold, a Class II or III could be included under the proposed rule, despite only operating 2% of the miles that the smallest Class I operated.[29]

According to data compiled by ASLRRA (and based on data reported to FRA), there are 16 Class II and III railroads that would exceed the proposed train mile threshold.[30] While many of these railroads would likely be brought covered by the rule under other

---

[27] See 89 Fed. Reg. at 88,508.

[28] See FRA, Accident Data as Reported by Railroads, available at https://safetydata.fra.dot.gov/OfficeofSafety/publicsite/on_the_fly_download.aspx.

[29] See id.

[30] See ASLRRA, 2023 EOD Report, https://www.aslrra.org/aslrra/document-server/?cfp=aslrra/assets/File/public/awards/2023/2023%20ASLRRA%20EOD%20Report.pdf

provisions, this provision would also encompass several regional operations that would not significantly affect the operation of the national rail network if impacted by a cyber incident.

Next, the NPRM proposes to include railroads with switching and terminal operations served by more than one Class I railroad.[31] This proposal has the potential to impact a far greater number of railroads than indicated by the NPRM's Regulatory Impact Analysis ("RIA"). Some of these operations—such as those in Chicago or St. Louis that serve many different Class I operators and function as key linkages between the largely separate eastern and western Class I freight networks—warrant inclusion under the NPRM. However, the proposed rule would also cover all switching and terminal railroads that serve multiple Class I railroads, including those small operations that provide switching services for rail-served industrial parks or other similar small-scale operations. For those railroads and their customers, access to multiple Class I partners is reflective of the advantages of partnering with different Class Is, depending on the nature of a given shipment; it should not suggest that these small switching operations represent a critical node in the freight network, or a volume of freight that is likely to be of national consequence in the event of a cyber incident.

Finally, TSA should consider modifying the rule's applicability to Class II and III railroads based on hosting Class I traffic.[32] This provision is written very broadly and, under the provisions of the existing security directives, it has been interpreted by some local TSA

---

[31] See 89 Fed. Reg. at 88,508.

[32] This language is already a part of 49 CFR 1580.101(c). See https://www.ecfr.gov/current/title-49/part-1580#p-1580.101(c).

staff to include short lines that merely host a physical interchange of cars with a Class I partner. The vast majority of Class II and III railroads host interchanges with their Class I partners, largely due to the advantages provided by performing interchange operations on short lines' relatively low traffic lines, or in order to permit the short line railroad to avoid having to maintain expensive interoperable PTC-equipped locomotives and back-office systems solely for interchange operations. In the past, TSA headquarters has helpfully provided guidance in certain cases; however, in order to ensure that the scope of the final rule does not expand beyond the stated intentions of TSA, it should clearly exempt from this category operations that are solely interchange.

VI. Additional Concerns

While the above concerns are among the highest priority for the Associations and their members, there are additional areas of the proposed rule that must be clarified or otherwise improved upon in order to create a final rule that is not overly burdensome and does not negatively impact railroad operations or security.

A. TSA Cybersecurity Lexicon

The TSA Cybersecurity Lexicon is defined as "a list of terms and their meaning applicable to cybersecurity requirements . . . available in a form and manner determined by TSA."[33] The NPRM goes on to propose that "TSA may update and revise the lexicon following the procedures . . . for amendments to security programs."[34] In other words, the Lexicon could change, without formal notice and comment, in a manner that forces an

[33] 89 Fed. Reg. at 88,552-23.

[34] Id.

otherwise compliant railroad out of compliance. This simply cannot be. Any changes to the final rule, including to definitions, must be subject to notice and comment rulemaking.

B. Definition of "Disruption."

Certain terms within the proposed rule would benefit greatly from a definition. For example, the word "disruption" (or "disruptions") appears more than 50 times within the NPRM, and yet no definition is provided. The Associations proffer that the definition must be a period of time that reflects a sustained inability to operate.[35]

C. Cybersecurity Assessment Plan

As noted above in Section I, the NPRM proposes that owner/operators annually conduct an enterprise-wide cybersecurity evaluation that would identify the current profile of cybersecurity compared to the target profile.[36] While it is stated that the CAP must be "sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls when evaluated against the CRM program requirements in this [NPRM]," it is unclear what the actual requirements of the CAP will be.[37] This problem is exacerbated by reference to "a form [to be] provided by TSA" and other unnamed "tools approved by TSA."[38] Without a fulsome explanation of the CAP process, a review of the TSA-provided form, and an understanding of what other TSA-

---

[35] Relatedly, the phrase "sustained disruption" is used with respect to pipelines elsewhere in the NPRM. It is unclear what this phrase means and whether this is intended to apply to railroads as well.

[36] Id. at 88,491.

[37] Id. at 88,561.

[38] Id.

approved tools are available, it is impossible to provide meaningful comments with respect to the CAP.

D. Cybersecurity Operational Implementation Plan

Per the NPRM, "owner/operators must make their COIP available to TSA in a form and manner prescribed by TSA."[39] However, the final rule must be elucidated to permit railroads to maintain the COIP, as well as any other security-related documents, at their physical locations, and reviewed by TSA through on-site visits. Any other method of review unnecessarily exposes the railroads to cybersecurity threats, in direct contravention of the intention of the proposed rule.

In addition, the COIP would require Cybersecurity Coordinators and the "accountable executive" to be listed, by name, and TSA must be alerted to any personnel changes within seven days.[40] The requirement that TSA have the names of the individuals serving in these roles does not meaningfully improve cybersecurity; indeed, as long as a railroad has a Cybersecurity Coordinator who is reachable at the contact information listed in the COIP, the names of the individual(s) serving should not matter. Instead, this proposed requirement would merely create unnecessary administrative work for railroad employees, as each personnel change will necessitate an update to the COIP; it should therefore be removed from the final rule.

---

[39] Id. at 88514. It is unclear whether the COIP is meant to mirror the Cybersecurity Implementation Plan ("CIP") presently proscribed by the operative security directive. Further, if the COIP is to replace the CIP, it is unclear what happens with the CIPs presently on file with the TSA. If the intention is for the CIPs to become null as of the effective date of the proposed rule, this must be clarified.

[40] Id. at 88530. The same is true of software and software versions.

E. Audits

The NPRM proposes that owners/operators conduct regular audits of their cyber risk management ("CRM") programs to evaluate effectiveness.[41] These audits would be required to be conducted by individuals who, or companies that, are "independent, i.e., do not have a personal, financial interest in the results of the assessment."[42] The rule must be clarified to ensure that a qualified railroad employee may conduct the audit. This will ensure that costs associated with the audit are kept to a reasonable minimum.

F. Backups or "Workarounds"

The Associations and their members are concerned that the proposed rule states "that the availability of backups or 'workarounds' should not be considered in determining whether an IT or OT system is a Critical Cyber System."[43] However, that proposal is contradictory to the concept of resiliency and contrary to the reason for a workaround existing. As such, this provision should be removed from the final rule.

Further, the proposed rule provides an owner/operator may only restore backups from previously identified systems. However, if an older, viable backup system can maintain service during a cybersecurity incident, railroads need to be able to use that backup without being in violation of the final rule.

Additionally, the rule would require that "all stored backup data is scanned with host security software to ensure the data is free of malicious artifacts before being used for

---

41 See id. at 88,488.

42 Id. at 88,491.

43 Id. at 88,516.

restoration."[44] This requirement would slow down a return to normal operations by requiring the scanning of equipment that is not online and therefore has not been exposed to risk. Simply stated, this proposal would cause unnecessary delay without cause.

G. Cybersecurity Training

The NPRM proposes that TSA-approved basic cybersecurity training must be provided to all employees, including contractors, with access to the IT or OT system, and additional training must be provided to cybersecurity-sensitive employees.[45] This requirement, as proposed, is overbroad, and more focused training would be appropriate. Training of employees without the appropriate level of administrative access to the IT/OT systems will create needless expense without corresponding advancements in operational safety or reliability.[46]

In addition, the requirement that training be provided within 10 days of onboarding, or within 60 days of approval of the COIP, is too short.[47] The Associations recommend a 30-day on-boarding period.

The rule would also require records retention of all training for five years, including for those individuals who are no longer employed at the railroad.[48] There is no need for railroads to incur this cost for former employees.

---

[44] Id. at 88,566.

[45] See id. at 88,521.

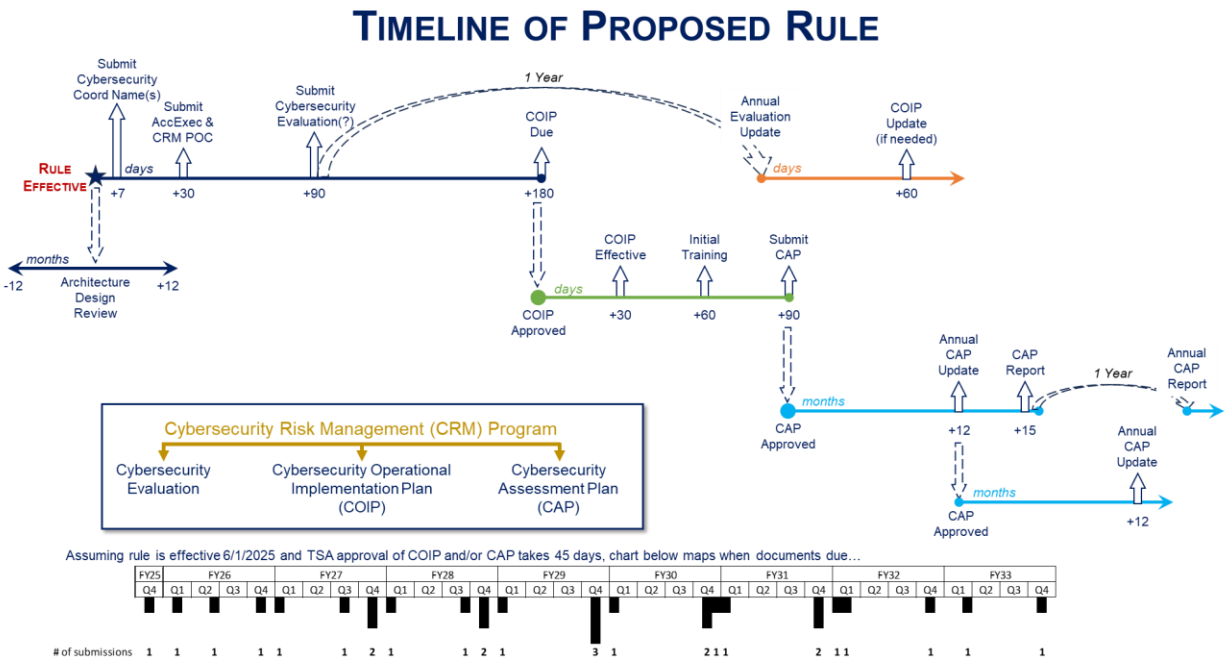
[46] At present, the TSA's present estimate for development of an 80-hour training program is far too low. It is not reflective of the costs involved for Class I railroads to modify their current programs, let alone the costs involved for many short line railroads to develop plans from scratch.

[47] See id.

[48] See id. at 88,549.

H. Reporting Timeline

The reporting timeline proposed by the NPRM is confusing and appears to be quite burdensome at times, with the potential for three or more reports to TSA required in a single quarter. An attempt to map out the timelines highlights these issues.



Accordingly, the Associations propose that TSA consider a revised schedule with a more regular cadence of submissions.

I. Physical Security

While the proposed rule is styled as a cybersecurity regulation, it also proposes to govern certain aspects of physical security**.** The definition for physical security in the NPRM includes measures that provide for the security of systems and facilities, as well as the persons in areas in, or near to, operations that could have their safety and security threatened by an attack on physical systems and assets, such as rail cars and stations.[49] Indeed, one individual reported being advised that the theft of a "porta potty" would need to be reported to TSA under the physical security requirements. This is an example of "mission creep" that can cause more harm than good.

CONCLUSION

TSA should amend the final rule as outlined above—with a particular eye towards correcting unclear or overly burdensome proposals as to governance, clarification as to the inclusion of PTC as a "critical cyber system," removal of the supply chain management proposal, and harmonization of the cybersecurity incident reporting requirements. The

[49] See id. at 88,502.

Associations and their members appreciate the opportunity to comment and express their concerns with respect to the proposed rule.

Respectfully submitted,

Kathryn D. Kirmayer
J. Frederick Miller Jr.
Amber L. McDonald
Association of American Railroads
425 Third Street, S.W., Suite 1000
Washington, DC 20024

Counsel for the Association of American Railroads

Sarah Yurasko
American Short Line and Regional Railroad Association
50 F Street N.W., Suite 500
Washington, DC 20001

Counsel for the American Short Line and Regional Railroad Association