

**BEFORE THE  
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE (NPPD)  
DEPARTMENT OF HOMELAND SECURITY**

---

**DOCKET NO. DHS-2017-0037:  
INFORMATION COLLECTION REQUEST  
CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)  
PERSONNEL SURETY PROGRAM**

---

**SUBMITTED BY THE  
ASSOCIATION OF AMERICAN RAILROADS  
AND AMERICAN SHORT LINE AND REGIONAL RAILROAD ASSOCIATION**

---

The Association of American Railroads (“AAR”) and the American Short Line and Regional Railroad Association (“ASLRRA”), on behalf of themselves and their member railroads, submit the following comments in response to the information collection request published by the Department of Homeland Security’s (“DHS”) National Protection and Programs Directorate (“NPPD”) pertaining to implementation and expansion of the Chemical Facility Anti-Terrorism Standards (“CFATS”) Personnel Surety Program (“PSP”).<sup>1</sup>

Under this program, DHS has mandated that covered “high risk” chemical facilities must ensure that persons with unescorted access to defined sensitive areas have undergone vetting against terrorist watch lists maintained by federal security and law enforcement departments and

---

<sup>1</sup> AAR is a national, non-profit trade association that represents the nation’s major freight railroads, smaller freight railroads, Amtrak, and commuter railroads. AAR’s membership includes freight railroads that operate 83 percent of the line-haul mileage, employ nearly 170,000 workers constituting 95 percent of those employed in the industry, and cumulatively account for 97 percent of the freight revenues of all railroads in the United States. AAR is the nation’s leading railroad policy, research, standard setting, and technology organization. AAR and its members are committed to operating the safest, most efficient, cost-effective, and environmentally sound rail transportation system in the world. AAR’s members create and implement a comprehensive security program to protect critical infrastructure, including transport of hazardous materials to and from chemical facilities. As such, AAR and its members are stakeholders directly impacted by DHS’s proposed information collection requirement.

The American Short Line and Regional Railroad Association (ASLRRA) is a non-profit trade association representing the interests of approximately 450 short line and regional railroad members and railroad supply company members in legislative and regulatory matters. Short lines operate 50,000 miles of track in 49 states, or approximately 38% of the national railroad network, touching in origination or termination one out of every four cars moving on the national railroad system, serving customers who otherwise would be cut off from the national railroad network.

agencies. From the initial stages of the rulemaking process that has produced this program, the railroad industry has maintained a consistent position – that the requirement should not pertain to railroad employees for lack of risk-based justification and that implementation will actually exacerbate security risk.

The proposed information collection request does not simply seek renewal of an existing procedure. Rather, if approved, the scope of data collected – by governmental and private sector entities – would expand dramatically. For this collection request calls for a vast increase in the application of the Personnel Surety Program from the current 200 chemical facilities by adding some 3,700 more at lower risk tiers – a 1850% increase.

This planned action is flawed in several material respects and, therefore, should not proceed.

### **I. This Notice Underestimates the Information Collection Burden**

The information collection notice underestimates the actual burden by failing to include and account for the impacts of the proposed vast expansion of information collection requests on railroads and other entities whose personnel visit the covered chemical facilities. Further, the manner of implementation of this program has already imposed and exacerbated these effects through the collection of unnecessary and burdensome information.

The Personnel Surety Program is implemented on a facility-by-facility, rather than company-wide, basis. This practice encourages duplicative processes for information collection and vetting and dramatically increases the burdens on railroads serving more than one company location. Rather than responding to one point of contact at a company, the railroads must field multiple, staggered information requests. Also, with the downplaying of some of the existing options to lessen the burdens on railroads and other non-employees (such as the option for real-time video monitoring as a means of escort), DHS has encouraged facilities to collect information that exceeds the legal requirements. In implementation, the emphasis has been almost wholly placed on requesting that third party entities, including railroads, submit personally identifying information on their employees to each chemical facility they may enter for vetting. As discussed further below, the application of this program and its information collection requirements to railroads is unnecessary and burdensome and actually produces the undesired effect of creating new security risk.

### **II. Lack of Risk-Based Justification for Application to Railroad Employees**

An inherent contradiction exists between the CFATS/PSP's terrorist watch list vetting requirement and railroads' record of compliance with pre-existing security regulations. Railroads meet Department of Transportation ("DOT") regulations that mandate inclusion in security plans of effective provisions for background vetting of railroad employees involved in transportation of hazardous materials. Further, through these plans and related efforts, railroads

implement and sustain security actions recommended by the Transportation Security Administration (“TSA”) on background checks, redress, and appeal.

With consideration of the quality of this vetting, and thorough, and recurring, risk assessments, DOT and TSA promulgated regulations on transport of hazardous and security sensitive materials that rely upon the diligence of well-trained railroad employees.<sup>2</sup> Addressing “Personnel Security,” the DOT regulation directs railroads to maintain in their required security plans, “Measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan.”<sup>3</sup> Railroad employees are integral to accomplishment of the other two required elements of the DOT-mandated security plans:

- “Measures to address the assessed risk that unauthorized persons may gain access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials covered by the security plan”;<sup>4</sup> and
- “Measures to address the assessed security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement.”<sup>5</sup>

Recurring audits conducted by officials with Federal Railroad Administration (“FRA”) headquarters, and by field inspectors assigned to and managed by the agency’s regional offices, validate railroads’ compliance with this requirement.

In particular, TSA’s regulations on secure transport of rail security sensitive materials, which include chemicals that are toxic-by-inhalation (“TIH”), depend on railroad employees to conduct multiple actions effectively, specifically:

- Security inspections of tank cars transporting rail security sensitive materials;<sup>6</sup>
- Secure and documented transfers of custody;<sup>7</sup> and
- Reporting of significant security concerns.<sup>8</sup>

Inspections conducted by TSA Transportation Security Inspectors – Surface (“TSI-S”) vindicate this confidence in the training, attentiveness, and diligence of railroad employees. Compliance with secure handling requirements has ranked consistently at 98 to 99% effectiveness. In 2016, per TSA’s annual report on risk reduction, railroads achieved a 99.7% level of compliance with the regulatory provisions on secure transport and handling of rail security sensitive materials.<sup>9</sup> On February 20, 2018, during a monthly teleconference held

---

<sup>2</sup> The relevant DOT regulatory provision is at 49 CFR section 172.802; the TSA requirements are set by 49 CFR section 1580.107.

<sup>3</sup> 49 CFR section 172.802(a)(1).

<sup>4</sup> 49 CFR section 172.802(a)(2).

<sup>5</sup> 49 CFR section 172.802(a)(3).

<sup>6</sup> 49 CFR section 1580.107.

<sup>7</sup> 49 CFR section 1580.107.

<sup>8</sup> 49 CFR section 1580.105.

<sup>9</sup> TSA – Annual Report on Risk Reduction Performance Measure (2016).

between TSA freight rail security officials and the security and law enforcement leads for freight and passenger railroads nationally, TSA's freight rail industry liaison announced that railroads had once again maintained an exceptional caliber of performance in 2017 – 99.43% level of compliance with the regulatory provisions on secure transport and handling of rail security sensitive materials.<sup>10</sup>

Throughout rail transportation, train crew members and other railroad employees have full access to tank cars transporting rail security sensitive materials, again including TIH chemicals. In neither risk assessments nor explanations of chemical security policies have DHS officials adequately explained why railroad employees of such proven reliability in assuring secure transport and compliance with federal regulations, again with access to the tank cars over hundreds of miles, are suddenly deemed suspect simply by crossing a fence line at a chemical facility.

- Railroad employees access chemical facilities for a limited period to accomplish a defined purpose – pick-up or delivery of rail cars and necessary security and safety inspections.
- As consistently recorded in field inspections by TSA surface transportation security inspectors, these types of actions are completed at an exceptional level of compliance with specific requirements on security inspections, secure transfer of custody, completion of necessary documentation, and reporting of significant security concerns.
- These actions are taken by railroad employees every day, without adverse incident, at chemical facilities nationwide.

The fundamental contradiction of application of CFATS/PSP to railroads' employees is not resolved by the decade-old risk assessment on which the program is based. Indeed, the age of the assessment is indicative of the scope of relevant security activities that have been disregarded in the development and implementation of the CFATS/PSP.

- That assessment has not been provided to security representatives of railroads or industry organizations.
- Based on its age, it could not consider railroads' exceptional record of compliance with security requirements that pertain to chemicals transported from and delivered to chemical facilities covered by the CFATS/PSP.
- A recurring theme – from proposal to promulgation of the requirements that necessitate changes to the security plans of designated “high risk” chemical facilities – has been the inadequate coordination by DHS/NPPD with TSA and DOT.
- As a result, the sound bases for the latter two organizations' reliance on railroad employees in meeting security requirements pertaining to transport of rail security sensitive materials to and from chemical facilities covered by the CFATS/PSP, and the vindication of that reliance in the exceptional caliber of performance recorded in audits and inspections by federal officials, have never been adequately considered by DHS/NPPD.

---

<sup>10</sup> Announcement – Transportation Security Administration – Rail Security Working Committee Monthly Teleconference February 20, 2018).

### **III. Compliance Exposes Employees' Personally Identifying Information, Needlessly Exacerbating Cyber Security Risk**

Compounding its other flaws, the CFATS/PSP needlessly escalates cyber risk. As chemical companies seek to meet the program's requirements, experience to date has demonstrated that the preferred means of compliance for chemical facilities is "Option 1 - Direct Vetting." Under this approach, some chemical companies are requesting that railroads submit personally identifying information (PII) on their employees to the hundreds of "high risk" chemical facilities they may have to enter as part of their rail transportation duties. The chemical facilities would then deliver this data to DHS for conduct of the terrorist watch list vetting.

A principal reason for this preference seems to be cost effectiveness and lesser administrative demands in comparison with the other available options. However, such a proliferation in handling and storage sites expands cyber attack opportunities and exposure of the data to compromise, in defiance of federal cybersecurity guidelines, notably:

- Measures recommended by DHS in the Cybersecurity Framework, jointly issued in February 2014 with the National Institute of Standards and Technology (NIST);<sup>11</sup> and
- Alerts and advisories issued by DHS's United States Computer Emergency Readiness Team.<sup>12</sup>

These well-founded sources urge the following types of actions for protection of personally identifying information (PII):

- Minimizing proliferation of PII – that is, the volume of locations to which such information is sent and maintained;
- Limiting uses of PII;
- Controlling access to PII – by such means as effective management of credentials for access, assuring that privileged users understand their roles and responsibilities, and recurring cybersecurity training and awareness initiatives; and
- Protecting PII as data-at-rest – through such means as computer network segregation, user access controls, training of those with access, restricted use of removable media, protective measures to mitigate the risk of data leaks or compromise, and implementation of a continuous improvement process for data protection.

The practical effect of the CFATS/PSP is to prompt chemical companies to request that railroads submit PII on their employees to each individual "high risk" chemical facility they may enter in the course of their duties in accepting, inspecting, and transporting rail tank cars for shipment of chemicals from origin to destination. The effect of this federally-mandated requirement directly contradicts sound, and federally recommended, cyber security practice – as it requires PII on thousands of railroad employees to be separately submitted to, and maintained at, nearly 4,000 chemical facilities. This proliferation of PII would expand greatly the opportunities for illicit cyber actors and others with malicious intent to obtain identifying

---

<sup>11</sup> NIST Cybersecurity Framework – Official Site: <https://www.nist.gov/cyberframework>

<sup>12</sup> United States Computer Emergency Readiness Team – Official Site: <https://www.us-cert.gov/>

information on railroad employees who access specifically identified chemical facilities. This needlessly created vulnerability for sensitive data would substantially exacerbate the kinds of security risks that the CFATS program is intended to mitigate.

#### **IV. Railroads' Steadfast Commitment to Security Is Well Demonstrated**

In the wake of the terrorist attacks of September 11, 2001, railroads' operations, law enforcement, and security officials developed the unified Security Management Plan that provides the foundation for coordinated efforts across the railroad industry and with government departments and agencies in the United States and Canada.

- Implemented in January 2002, the industry plan applies a unified, risk-based, and intelligence-driven approach to rail security and risk mitigating actions.
- Dedicated industry security coordinating committees, led by railroads' physical and cyber security leads, manage implementation of the plan, including a persistent emphasis on identifying opportunities to enhance capabilities and overall effectiveness in addressing physical and cyber threats.
- The plan's four alert levels call for increasing security measures, both physical and cyber, driven by assessments and analyses of threats and related indicators of concern.
- Recurring training sessions and awareness initiatives with railroad employees ensure their understanding of their roles in implementing security plans and measures and of indicators of significant security concern that warrant timely reporting. During 2015 and 2016, railroads cumulatively trained more than 160,000 employees in security awareness.
- Recurring exercises test the plan's effectiveness in realistic physical and cyber scenarios. Exercises are held within railroads, in conjunction with local law enforcement and emergency response organizations, and industry-wide, the latter on an annual basis with participation by federal security and law enforcement agencies in the United States and Canada. Again, during 2015 and 2016, railroads cumulatively conducted and participated in more than 370 exercises related to security preparedness.
- Results of these exercises, and experience with actual incidents, are applied in a continuous improvement process to enhance capabilities, coordination, and protective measures.

Timely sharing of relevant and actionable intelligence assessments, analyses, and advisories, through consistent and effective procedures, is essential. It supports sustained security awareness, informed vigilance, and proactive implementation of planned security measures and actions to narrow risk profile, afford opportunities for prevention, and mitigate potential consequences.

- Industry-defined intelligence requirements drive government security assessments and analyses of threats to railroads.
- Through the Railway Alert Network (RAN), the industry's security information center, and the work of members of dedicated physical and cyber security committees, railroads effectively apply the intelligence analyses received from government security and intelligence agencies, as well as other reliable sources, to inform vigilance, enable

decisions on security measures and related activities, and build and sustain layers of security.

- Further, the industry works closely with the FBI's National Joint Terrorism Task Force (NJTTF) and Rail Security Program (RSP) through an experienced railroad police special agent, detailed full-time to these components. The RSP includes Rail Liaison Agents (RLA) assigned to each of the Joint Terrorism Task Forces (JTTF) based at FBI Field Offices. RLAs share intelligence and security-related information in their assigned areas with law enforcement and security officials for freight and passenger railroads

The scale of this collective effort, which includes more than 130 railroads that have adopted and implemented the industry security plan, demonstrates the railroad industry's longstanding commitment to a well-planned, coordinated, and risk-based approach to security.

## V. Conclusion

This information collection requirement for the CFATS/PSP, and its proposed expansion nearly twenty-fold, should be declined for lack of risk-based justification for its scope of application and flaws in implementation that are undermining the program's stated objectives.



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



Jo Strang  
Senior Vice President – Safety and  
Regulatory Policy  
American Short Line and Regional  
Railroad Association