TESTIMONY OF

THOMAS L. FARMER

CHAIR

CROSS-SECTOR COUNCIL

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

BEFORE THE

U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING ON ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE: THREATS, VULNERABILITIES, AND SOLUTIONS

MAY 18, 2016

Good morning, Mr. Chairman and Members of the Senate Homeland Security and Government Affairs Committee. I am Tom Farmer, Assistant Vice President for Security for the Association of American Railroads.

Today, however, I am testifying in my capacity as the Chairman of the Cross-Sector Council of the Partnership for Critical Infrastructure Security (PCIS). The PCIS is a representative forum, established at the private sector's initiative, which facilitates consultations, information sharing, and coordinated effort across the critical infrastructure sectors and sub-sectors and with the federal government. We also work with the State, Local, Tribal, and Territorial Government Coordinating Council, the Regional Consortium Coordinating Council, and the National Council of Information Sharing and Analysis Centers.

PCIS dates from 1999, when it was established by the private sector to address priorities defined in Presidential Decision Directive 63 (*Critical Infrastructure Protection)* — most notably, to foster partnering with government for mitigation of security risks. While the representatives of the respective sectors and sub-sectors have changed over time, the commitment by members of the PCIS to cooperative efforts to enhance preparedness for all hazards and emergencies has not wavered.

The adaptive structure maintained by the private sector has enabled the PCIS Cross-Sector Council to meet the requisites of Presidential directives issued following the terrorist attacks of September 11, 2001, and of the National Infrastructure Protection Plan (NIPP), as first implemented in 2006 and in later updates. (The most recently updated is *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience).* Consistent with the organizing approach established under the NIPP, the Cross-Sector Council is comprised of the Chairs, Co-Chairs, Vice Chairs, and Designated Representatives of the Sector Coordinating Councils of each of the critical infrastructure sectors and sub-sectors.

Regular consultations occur between members of the PCIS Cross-Sector Council and federal officials, especially from the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence, and other federal agencies responsible for various critical infrastructure sectors. Some meetings occur regularly; others are driven by threats, incidents, or emergencies of interest to the sectors' representatives.

To afford the opportunity to engage with federal government officials for the purpose of achieving consensus on joint priorities and actions to advance critical infrastructure security, protection and resilience, some joint meetings between the PCIS Cross-Sector Council and representatives of federal departments and agencies are convened under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework.

The objectives, accomplishments, and continuing efforts of the PCIS Cross-Sector Council and its members are reflected in three categories: (1) unified priorities for action defined with DHS and its federal partners; (2) sector-based interaction with government components; and (3) cross-sector cooperation on interdependencies. I discuss each of these in turn below.

Unified Priorities for Action with Federal Partners

Four fundamental priorities drive the PCIS Cross-Sector Council's unified efforts with DHS and its federal government partners in the critical infrastructure protection and resilience mission:

(1) Timely Sharing of Actionable Intelligence:

The first priority is to ensure timely sharing of actionable intelligence and related security information on developing threats and concerns. In this vital area, PCIS members proposed a Joint Threat and Security Intelligence Engagement Group to leverage the existing cross-sector councils established by government and industry in the implementation of the National Infrastructure Protection Plan.

The objective is to ensure common, and sustained, awareness across sectors and sub-sectors – within industry, in supporting Information Sharing and Analysis Centers, and within governmental Sector Specific Agencies. Sharing practical and applicable threat intelligence and security information creates opportunities to narrow risk profiles through informed vigilance and, if warranted, heightened security measures.

The effectiveness of this engagement process was proven in a national communications exercise held November 10, 2015. Representatives of the government and industry cross-sector councils ratified the structure and procedures during a joint meeting on November 13. Within a matter of hours, the horrific terrorist attacks in Paris necessitated activation of the engagement group for its intended purpose – timely sharing of accurate information on developments and the threat and security implications for the United States.

Recognizing that at times the relevant intelligence and security information may be classified, the PCIS Cross-Sector Council proposed two significant enhancements to government procedures.

First, we leveraged the existing video-teleconferencing capabilities in state fusion centers[1] and field offices of federal agencies to enable secure sharing of classified information. This proposal sought to eliminate the inordinate delays and excessive costs that resulted from the recurring practice of calling private sector representatives to Washington, DC, for classified briefings and discussions on potential security threat or the implications of physical or cyber-attacks. There is substantial progress to report.

On April 26, 2016, DHS's Offices of Infrastructure Protection and Intelligence and Analysis partnered with a group of PCIS Cross-Sector Council representatives and officials at state fusion centers to hold a classified briefing via secure video teleconference. Participating fusion centers included Colorado, Kentucky, New York, and Wisconsin (Madison and

[1] State fusion centers are locally owned and operated facilities that serve as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between government, tribal, and private sector partners. DHS considers them to be the primary conduit between frontline personnel, state and local leadership, and the rest of the homeland security enterprise.

Milwaukee). DHS hosted the conference from its offices in Arlington, Virginia. This initial test proved the concept.

A second similar exercise will be held by early July 2016, with the aim of reaching representatives of each of the critical infrastructure sectors and sub-sectors nationwide. With this capability, what had formerly taken weeks to accomplish in multi-lateral sharing of classified information can now occur within just a few hours, ensuring awareness and enabling more timely actions to narrow risk profiles.

The second significant enhancement to government procedures we proposed is the concurrent development of an unclassified "tear line" during production of a classified assessment or analysis to enable participants to bring actionable information to their respective sectors. In the absence of appropriate security clearances and need-to-know, the classified information received cannot be shared. But to ensure the objectives in holding the classified meeting are met, an unclassified version enables participants to bring information to their sectors that can be applied to inform vigilance and, as warranted, proactive protective or preparatory measures.

(2) Draw and Apply Lessons Learned

The second priority is to draw lessons learned from the numerous exercises and regional risk and resiliency assessments conducted or sponsored by DHS. A wealth of information and experience has been gained from the conduct of National Level Exercises (NLEs), Cyber Storm exercises[2], and applications of the Regional Resiliency Assessment Program. Too often, however, the conduct of the exercise or the assessment itself is the performance measure rather than an analysis of results and lessons learned to identify any recurring deficiencies in capabilities, coordination, or performance. The identified concerns could then inform joint priorities for action by the government and industry cross-sector councils. We are working with government partners to achieve this outcome.

(3) Enhance Risk Management

The third priority is to enhance cyber threat analysis and its effectiveness as a risk management tool. DHS and FBI have gained extensive experience and insights as they've responded to cyber breaches and threats and disseminated indicators of concern. This wealth of information on cyber tactics employed and on gaps in preparedness allows recurring analysis of this information to inform cybersecurity risk mitigation by highlighting:

- Tactics that are most commonly employed to gain illicit access to networks and systems;
- Vulnerabilities in targeted systems and networks most frequently exploited;
- Indicators of these illicit activities most often noted in post-incident analyses that were missed or disregarded; and

[2] Cyber Storm refers to biennial DHS exercises designed to strengthen cyber preparedness in the public and private sectors. The most recent exercise took place March 8-10, 2016.

- Protective measures most often found lacking or absent that could have made a difference.

As a comparative reference, Australia's equivalent to the United States Computer Emergency Readiness Team (US-CERT) conducted such an analysis and found, "at least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following" four mitigation strategies. This determination, shared publicly via the ASD's website, informs effective cyber risk management decision-making for private sector entities in Australia.

Applying information that is already available can enable collective improvement, across the sectors, in defeating the most common tactics and redressing frequently exploited vulnerabilities and gaps. Significantly, DHS has commissioned a pilot program focused on these analytical priorities for the Transportation Sector, with the goal of applying lessons learned in products for sharing across sectors.

(4) Outreach – Early and Often

The fourth priority is early and regular outreach and coordination on proposed homeland security and preparedness strategies and programs, on preparedness initiatives, and on defining objectives to enhance practices and procedures.

At times, private sector input has been sought after many months of effort within government when, practically, the opportunity to shape or influence the finished product is substantially diminished. Yet, the strategies, programs, and initiatives often entail some level of action by private sector entities. More effective and sustainable outcomes are achieved when there is, from the outset, a common understanding of purposes and goals and opportunities for industries to provide relevant information and context based on their knowledge of and experience in their respective sectors.

Sector-Specific Interaction with Federal Partners

The second main category of activity by PCIS members is in their sector-specific interaction with government components. Frequently, these interactions have produced outcomes beneficial across the critical infrastructure community. For example:

- For enhanced cybersecurity, the Defense Industrial Base Sector partnered with the Department of Defense and DHS in an innovative program to share classified indicators of potential threats with private corporations. The success of this initiative prompted expansion to other sectors through a program managed by DHS. The productive outcome has enhanced awareness and opportunities to implement effective protective measures.
- Engagement by DHS officials with representatives of the Commercial Facilities and Retail Sectors in the aftermath of the terrorist attack at Westgate Mall in Nairobi, Kenya, in September 2013, produced a regionally applied training initiative that focused on indicators of concern, protective measures, and immediate response actions

for potential active shooter threats at malls, hotels, and other retail venues. This cooperative effort led to quarterly consultations on classified reporting on security threats and incidents by DHS and Commercial Facilities Sector representatives. This initiative has now been expanded to encompass representatives of other industry sectors. The collective group of government and industry representatives review information classified at up to the Top Secret level for broader cross-sector relevance and application and for opportunities to reduce classifications and produce unclassified advisories.

- In view of the persistent threat posed by active shooter incidents, representatives of multiple industries partnered with the DHS and FBI to develop a comprehensive training program on prevention and mitigation. The prevention element leverages insights gained from investigations of these types of incidents to highlight recurring behavioral indicators that have preceded a mass shooting attack. The mitigation component focuses on immediate actions that people at a targeted facility or area should take to protect themselves and others and to facilitate an effective law enforcement response. The application of this program in Washington, DC, in April 2016 drew wide participation by area law enforcement departments and security leads for educational institutions, corporations, trade associations, and other private sector entities.

Cross-sector Cooperation

Finally, the third main category of activity facilitated by PCIS is cross-sector cooperation. The regular interaction of industry representatives through meetings, consultations, coordination, and information sharing within the PCIS Cross-Sector Council fosters connections that yield benefits in expanded and enhanced cooperative efforts to address priorities and concerns defined in each of the sectors. As representative examples:

- PCIS coordinated a thorough assessment to identify interdependencies among critical infrastructure industries.

- The National Council of Information Sharing and Analysis Centers has engaged with PCIS sector representatives to conduct cross-sector exercises, using realistic physical and cyber threat scenarios that seek to enhance information sharing and coordinated efforts.

- The Electricity Sector has proactively engaged colleagues in the Communications, Information Technology, and Transportation Sectors in cooperative efforts to enhance the resilience of electrical power generation and transmission in the face of natural and man-made threats. Cross-sector exercises have tested plans and procedures for cooperative responses to mitigate effects of disruptions to availability of electrical power and facilitate more timely and efficient restoration actions.

- The Commercial Facilities Sector has provided cross-sector partners access to facilities designed for greater resilience in areas affected by emergencies.

- Entities within the Transportation Sector, notably the Rail and Highway and Motor Carrier sub-sectors, have assisted entities within the Communications Sector following major storms and other natural hazards in gaining access to infrastructure for response and recovery actions.

Again, the activities outlined above are representative examples. The full scope of effort is substantially broader, reflecting a fundamental strength of the critical infrastructure protection and resilience mission. Corporations, companies, and associations across industries are dedicating staff, resources, and investment to cooperative efforts across sectors and with government in a shared commitment to critical infrastructure protection and resilience. The sustained emphasis is on identifying opportunities to improve and proposing the solutions to transform the opportunities into productive and sustainable outcomes.

On behalf of the colleagues across sectors for whom I am privileged to serve as a representative and spokesperson, thank you for this opportunity to address their level of commitment and the scope and effectiveness of their efforts.