Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

Section 10(b) Report

TSA's Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework

EO 13636, Improving Critical Infrastructure Cybersecurity, directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework to reduce cyber risks to critical infrastructure. This report describes TSA's approach to encouraging voluntary adoption of the Framework.

While TSA has authority to regulate cybersecurity in the transportation sector should the threat so warrant, it has pursued collaborative and voluntary approaches with industry since 2010. TSA and its industry partners established the Transportation Systems Sector Cybersecurity Working Group (TSSCWG) to advance cybersecurity across all transportation modes. One of the first actions of the TSSCWG was to create a cybersecurity strategy. The strategy, completed in mid-2012, stated, "the sector will manage cybersecurity risk through maintaining and enhancing continuous awareness and promoting voluntary, collaborative, and sustainable community action." Government and industry actions to implement the strategy include increased information sharing to enhance community awareness of cyber threats, raised awareness of incident reporting procedures and channels, improved access to training resources, and notice to the community of cybersecurity best practices and standards. TSA provides cybersecurity pamphlets, a weekly newsletter, cybersecurity exercise support, and incident-specific threat briefings. DHS facilitates the Cybersecurity Assessment and Risk Management Approach (CARMA) for companies requesting assessments. The American Public Transportation Association encourages use of its voluntary standards for security of control and communications systems in transit environments. Additional initiatives include:

- TSA will host the second TSSCWG-sponsored cybersecurity-focused Intermodal Security Training and Exercise Program (I-STEP) exercise in August 2014.

- The Surface Transportation, Public Transit, and Over-the-Road-Bus Information Sharing and Analysis Centers (ISACs) publish and disseminate a Daily Open Source Cyber Report and Priority Cybersecurity-related Messages.

- The TSSCWG is developing implementation guidance for adoption of the NIST Framework.

In aggregate, the increased level of cyber threat information sharing and cybersecurity awareness provides a growing incentive for industry to adopt the security measures in the NIST Cybersecurity Framework.