TRANSPORT SECURITY
UNIFIED STAKEHOLDERS GROUP

TSUSG PC 9

Status: Ongoing

Fact Sheet

Priority—Cybersecurity issues and mitigation options (review cybersecurity and GPS spoofing/jamming approaches and vulnerabilities and develop recommendations for consideration by TSUSG)

Status and Mission

This PC is established to address the growing need for robust cyber-security measures across the transportation ecosystem, particularly in the handling and movement of radioactive materials. The committee serves as a collaborative platform for industry experts, government partners, and regulatory bodies to identify risks and develop actionable solutions. This PC focuses on bringing awareness and providing cyber-security resouces through the exploration of multi-industry defensive technologies. These resources aim to identify vulnerabilities, improve preparedness, and foster collaboration among stakeholders. Key areas of risk under consideration include:

- Cyber-security Awareness: Evaluating the effectiveness of cyber-security standards programs for personnel involved in transportation operations.
- Supply Chain Risks: Addressing vulnerabilities introduced by thrid-party contractors, freight forwarders, and suppliers.
- Route and Shipment Planning: Identifying risks related to GPS spoofing, route planning software vulnerabilities, and unauthorized access to shipment schedules.
- Technology Integration: Examining the security implications of geofencing, GPS, remote disabling technologies, and other connected systems.
- Incident Response: Testing organizational readiness for cyber incidents such as ransomware attacks, data breaches, or system outages during transport.
- Data Sharing and Communication: Ensuring secure and appropriate distribution of sensitive shipment information to authorized parties.
- Regulatory Compliance: Assessing alignment with cyber-security standards and identifying gaps in compliance with national and international regulations.
- Safe Havens and Emergency Protocols: Reviewing procedures for emergency stops and the use of designated safe havens in transit.
- Testing and Validation: Exploring opportunities for live testing of anti-cybersecurity technologies in controlled environments.
- Other…

Consideration will also need to be given to means by which cybersecurity can be detected and mitigated in all the situations previously identified. Included in this work is a review of all existing technologies and of new

TRANSPORT SECURITY
UNIFIED STAKEHOLDERS GROUP

TSUSG PC 9

Status: Ongoing

Fact Sheet

Priority—Cybersecurity issues and mitigation options (review cybersecurity and GPS spoofing/jamming approaches and vulnerabilities and develop recommendations for consideration by TSUSG)

Contact Information
Email: tsusg@ornl.gov
www.tsusg.ornl.gov

Last Revised
January 2025

technologies under development by members of TSUSG, including national labs, the Office of Radiological Security, and other research and development organizations.

A final component of this PC is to identify opportunities where those developing anti-cybersecurity technologies can work with the ultimate users of this technology (all within TSUSG membership) to identify practical needs and limitations and to identify opportunities for testing of the technology through to the point of commercial production of such technology.

Comprehensive records of work, scenarios, results, and opportunities should be kept for future reviews and planning related to cybersecurity risks and controls.