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 will use all means available to identify real and potential cybersecurity risks associated with planning for, conducting, and shipping/receiving radioactive sources. Consideration should be given to all shipment related work where cybersecurity could be a risk, including but not limited to the following:

- Shipper/customer (end-use location) shipping and receiving planning (scheduling, loading/unloading [with and without third parties]), movement of containers at destination (use site, port, consolidator), etc.)
- Source packaging/containment
- Regulatory approvals/import/export notifications
- Freight forwarder involvement
- Route planning
- Approval process
- Carrier preparation (single vs. multiple drivers, training, communications during preparations, etc.)
- Loading of containers onto truck and subsequently off of truck at destination or where mode is changed (e.g., road transport to ocean vessel)
- Distribution of shipment information to functional groups with a need to know
- Transport security plans
- Police escorts
- Truck/trailer technology (geofencing, GPS, multiple communication capabilities, remote disabling, etc.)
- Multiple driver integration and transfers
- Safe havens
- Third-party involvement in transport, loading, and unloading process
- 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
June 2022

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.