TSA Surface Operations Overview

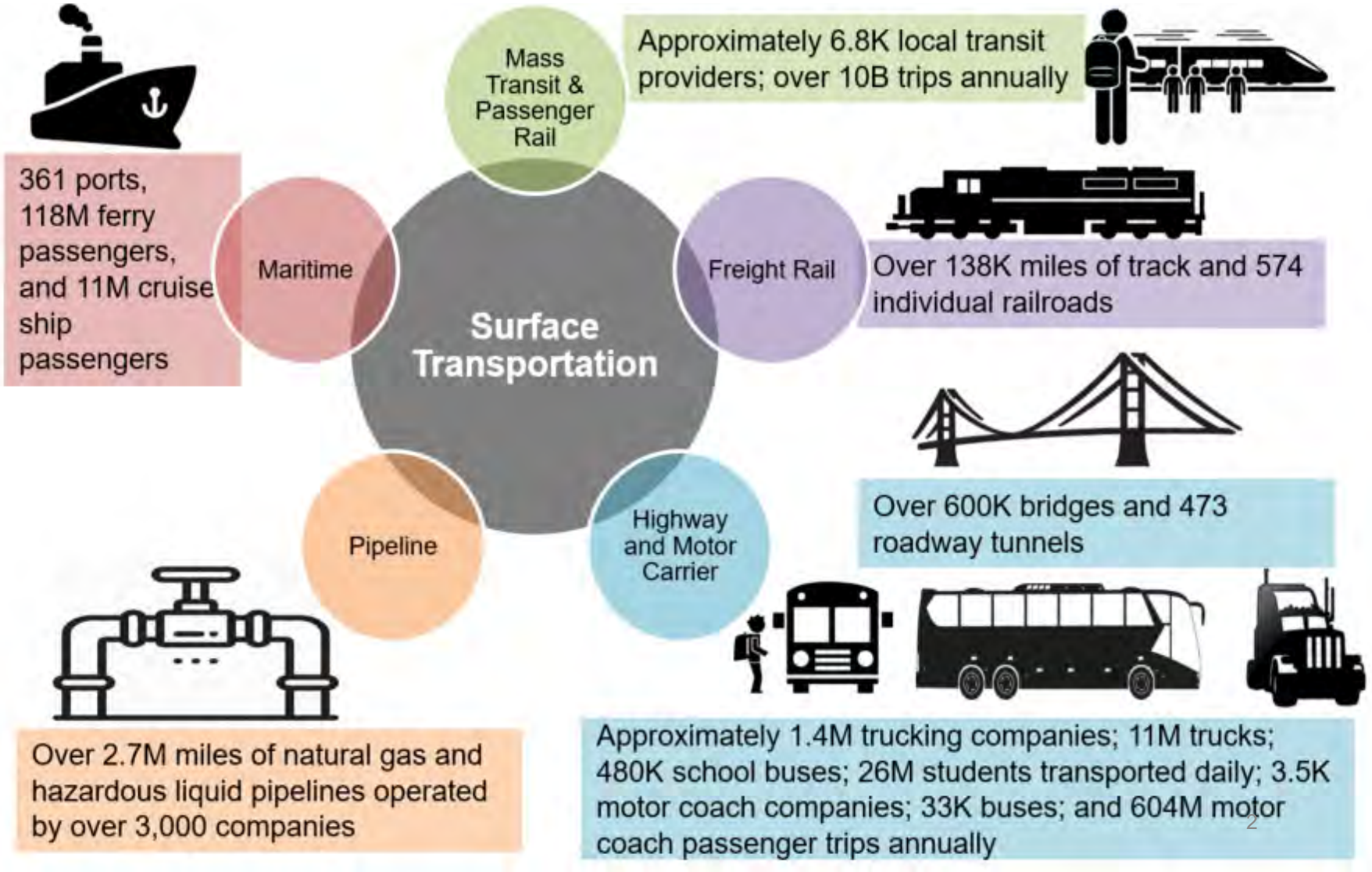
Ronald Pavlik
Deputy Assistant Administrator,
Surface Operations

April 7, 2022

Surface Transportation: Areas of Responsibility

Cybersecurity

Like physical security, the cybersecurity threat environment requires a comprehensive approach to risk management across the surface modes. It is vital to protect the IT/OT systems from cyber threats across all surface modes.



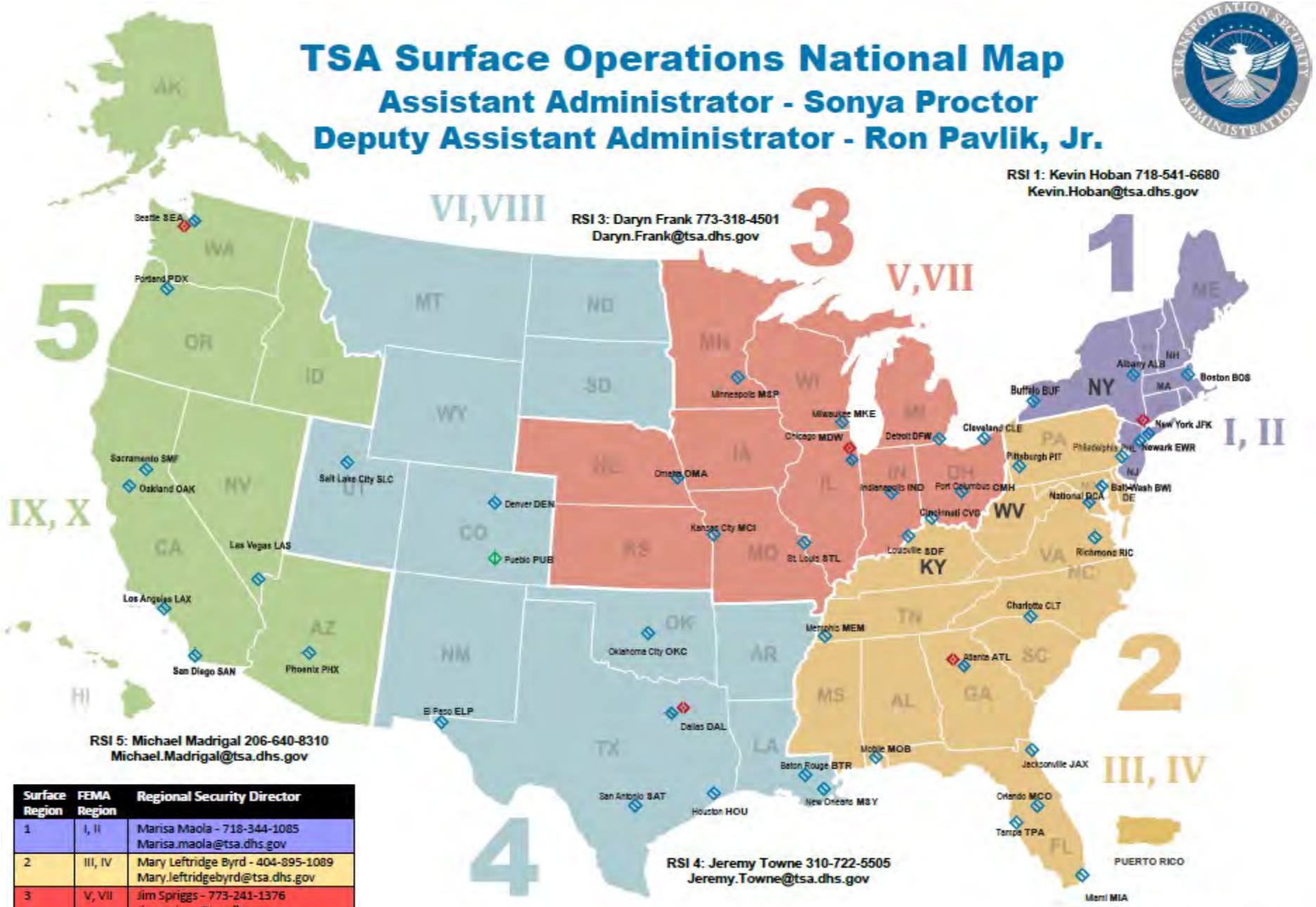
Comparison of Transportation Modes

	Aviation	Surface
 Regulatory Environment	Heavily regulated for security	Limited regulations for security; most objectives achieved through collaboration and voluntary compliance
 Annual Volume of Passengers/Ridership	927 million system wide scheduled service passengers (domestic and international)	Approximately 10 billion trips on public transportation
 Annual Movement of Cargo Shipments	Approximately 7 million tons carried	Approximately 14 billion tons carried by Truck, Rail, and Maritime combined
 Security Environment	Security screening provided by Federal personnel or Contract Screeners	Security provided by operators and local law enforcement
 Vetting of Passengers	Travelers are known; Secure Flight vetting	No vetting of travelers using surface transportation systems
 Operating Environment	Closed, restricted operating environment	Vast and open by nature operating environment

TSA Surface Operations National Map

Assistant Administrator - Sonya Proctor

Deputy Assistant Administrator - Ron Pavlik, Jr.



RSI 1: Kevin Hoban 718-541-6680
Kevin.Hoban@tsa.dhs.gov

RSI 3: Daryn Frank 773-318-4501
Daryn.Frank@tsa.dhs.gov

RSI 5: Michael Madrigal 206-640-8310
Michael.Madrigal@tsa.dhs.gov

RSI 4: Jeremy Towne 310-722-5505
Jeremy.Towne@tsa.dhs.gov

RSI 2: Curt Secrest 904-874-7224
Curt.Secrest@tsa.dhs.gov

Surface Region	FEMA Region	Regional Security Director
1	I, II	Marisa Maola - 718-344-1085 Marisa.maola@tsa.dhs.gov
2	III, IV	Mary Leftridge Byrd - 404-895-1089 Mary.leftridgebyrd@tsa.dhs.gov
3	V, VII	Jim Spriggs - 773-241-1376 Jim.spriggs@tsa.dhs.gov
4	VI, VIII	Mel Carraway - 703-342-2523 Melvin.carraway@tsa.dhs.gov
5	IX, X	James Duncan - 206-288-7815 James.G.Duncan@tsa.dhs.gov

◇ Surface Field Office
◇ Regional Security Director Office
◇ Surface Transportation Security Readiness Facility

2/28/2022

The Evolving Cyber Threat Environment

- With the current invasion by Russian forces on Ukraine there is increasing tension on Russian relationships with other countries, such as the US.
- The current threat environment that the U.S.A has to face is preparing for and protecting against potential and current Russian cyber attacks.
- Current threat intel is being gathered primarily from open-source tools and from groups like TSA's I&A.
- In addition to the Russian threat, multiple nation state actors continue to look for ways to exploit vulnerabilities in the US and are prioritizing remote access, data theft and ransomware.

The Evolving Cyber Threat Environment

- CISA provides and maintains an updated list of known exploitable vulnerabilities that sector partners may be vulnerable to.
- FBI and CISA have released a number of Joint Cybersecurity Advisories.
  - Joint Cybersecurity Advisory: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector (March 2022)
  - Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (March 2022)

TSA's Security Directive Authority

- In response to the ongoing cybersecurity threat to pipeline systems, TSA used its authority under 49 U.S.C. 114 to issue security directives (SDs) to owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.
- 49 U.S.C. 114(*l*)(2)(A) authorizes TSA to issue emergency regulations or security directives without providing notice or public comment where "the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security. . . ."
- Security directives issued pursuant to the procedures in 49 U.S.C. 114(*l*)(2) "shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Transportation Security Oversight Board or rescinded by the Administrator."

Pipeline Security Directive No. 1

- On May 26, 2021 TSA issued a Security Directive (Pipeline-2021-1)
- The SD is applicable to the owners and operators of hazardous liquid and natural gas pipelines that have been identified as critical by TSA.
- The SD requires three actions:
    1) Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 12 hours;
    2) Appoint a Cybersecurity Coordinator and at least one alternate to be available 24/7 to coordinate with TSA and CISA; and
    3) Conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation.

- This SD was effective as of May 28, 2021, is set to expire on May 28, 2022, and was ratified by the Transportation Security Oversight Board (TSOB) on July 3, 2021.

Pipeline Security Directive No. 2

- Security Directive Pipeline-2021-02 (SD-2) was effective on July 26, 2021
- The SD is applicable to the same group of critical pipeline Owner/Operators covered by the first SD
- The SD requires three major actions-
    1) Implement critically important mitigation measures to reduce the risk of compromise from a cyberattack;
    2) Develop a cybersecurity contingency/response plan; and,
    3) Test the effectiveness of cybersecurity practices through an annual cybersecurity architecture design review.

- SD was effective as of July 26, 2021 and is set to expire on July 26, 2022. The TSOB ratified the SD on August 4, 2021

Rail Security Directive

- In December 2, 2021, TSA issued two SDs that require higher-risk freight railroads, passenger rail, and rail transit operators to:
  1) Designate a cybersecurity coordinator, to be available 24/7;
  2) Report cybersecurity incidents to CISA within 24 hours;
  3) Develop and implement a cybersecurity incident response plan; and
  4) Complete a cybersecurity vulnerability assessment.

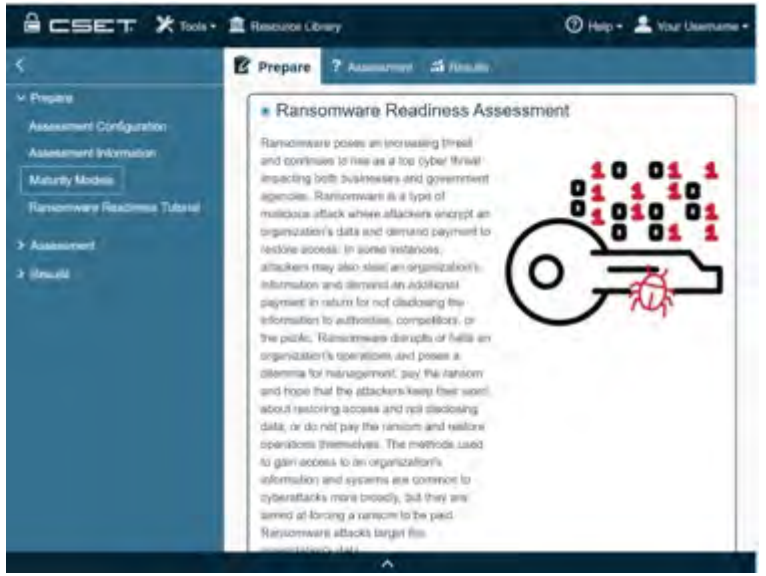
- An Information Circular was issued on December 2, 2021, for lower-risk surface entities recommending the same actions. Lower-risk stakeholders included:
  1) Freight Rail
  2) Passenger Rail
  3) Rail Transit
  4) Bus Transit
  5) Over-the-road buses

Self Evaluation Tool

Cybersecurity Evaluation Tool (CSET)

This is a free to use, TSA invested tool, which offers a Ransomware Readiness Assessment (RRA) module focused on best practices on preparation and response, where an organization can gauge their ransomware readiness posture against current best practices.

- TSA version available March, 2022



5N5 | Cybersecurity Workshop

TSA 5N5 CYBERSECURITY WORKSHOP

WORKSHOP GOALS

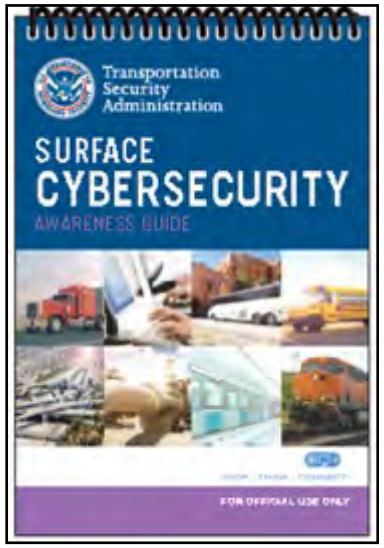
- **Provide cybersecurity resources and programs**
- **Discuss best practices and lessons learned associated with implementing cybersecurity measures**
- **Provide five nontechnical actions that can be implemented in five days ("5N5") that will enhance the organizations' cybersecurity posture**

"5N5" NONTECHNICAL CYBERSECURITY ACTIONS

Surface Cybersecurity Resources Offered to Stakeholders

TSA Surface Transportation Cybersecurity Resource Toolkit

TSA developed a collection of resources and programs for Small & Midsize Business (SMB) to offer guidance on how to incorporate "Cyber Risk" into small and midsize transportation systems' existing risk management and governance processes for



Surface Transportation Cybersecurity "Pocket" Awareness Guide

TSA developed a small "pocket-sized" guide for frontline employees to outline the types of threats most commonly found in cyberspace and explain how transportation systems can protect their data, computer systems, and personal information.

"No-Cost" Cybersecurity Resources for Surface Transportation Systems handout

Provides a list of cybersecurity programs and documents for Surface Systems Sector Industry Stakeholders can use to reduce their cybersecurity risk and increase their cyber resilience.

CISA Shields Up

- Products that we've promoted to assist surface stakeholders in response to recent cyber threats.
  - Known Exploited Vulnerabilities Catalog
  - Ransomware Guide
  - CISA's free cyber hygiene services
  - Cybersecurity Advisories (CISA and Joint)
  - Steps You Can Take To Protect Yourself & Your Family
    - Implement multi-factor authentication on your accounts
    - Keep software up-to-date
    - Think before you click (Phishing awareness)
    - Use strong passwords
  - Emergency Communication Resources

More Information/Contact Us

- Please visit https://www.tsa.gov/for-industry to obtain a copy of the Cybersecurity Toolkit or to learn more about other resources TSA offers.

- Email STSIP@tsa.dhs.gov or contact your local TSA Surface Field Offices to request additional materials or to schedule a 5n5 Cybersecurity Workshop.