FTA
FEDERAL TRANSIT ADMINISTRATION

Cybersecurity Awareness for Transit Agencies Webinar

October 24, 2023

U.S. Department of Transportation
Federal Transit Administration

Webinar Overview

This webinar will discuss FTA and CISA cybersecurity resources available to transit agencies and provide information on cyber hygiene, ransomware guidance and support to transit agencies available through CISA.

Speakers

- FTA's Office of Transit Safety and Oversight
  - Joe DeLorenzo – Associate Administrator and Chief Safety Officer
  - Bridget Zamperini – Safety and Security Specialist
  - Jeremy Furrer – Safety Policy and Promotion Division Chief
- DHS's Cybersecurity and Infrastructure Security Agency (CISA)
  - Rahul Mittal – Region III Cybersecurity Advisor

FTA Cybersecurity Resources

Bridget Zamperini
Safety and Security Specialist
Office of Transit Safety and Oversight

Cybersecurity Assessment Tool for Transit (CATT)

FTA published an open-source CATT tool on February 10, 2023, which assists small and mid-sized transit agencies in self-assessing their cybersecurity preparedness

CATT has three primary components:

- Data collection form
- Resulting report produced given data input from transit agency
- Resource guide on how to begin practices

CATT provides an on-ramp for agencies to identify key practices of a modern cybersecurity program with a self-assessment that uses Department of Homeland Security's Cyber Resilience Review as a basis and aligns with National Institute of Standards and Technology framework

Cybersecurity Resources for Transit Agencies

FTA's Cybersecurity Resources

Cybersecurity Resources for Transit Agencies

https://bit.ly/3AQQWqe

Contact

Bridget Zamperini
Safety and Security Specialist
for Transit Safety and Oversight
Federal Transit Administration
bridget.zamperini@dot.gov

CISA Overview

Rahul Mittal
Cybersecurity Advisor– Region III
Cybersecurity and Infrastructure Security Agency

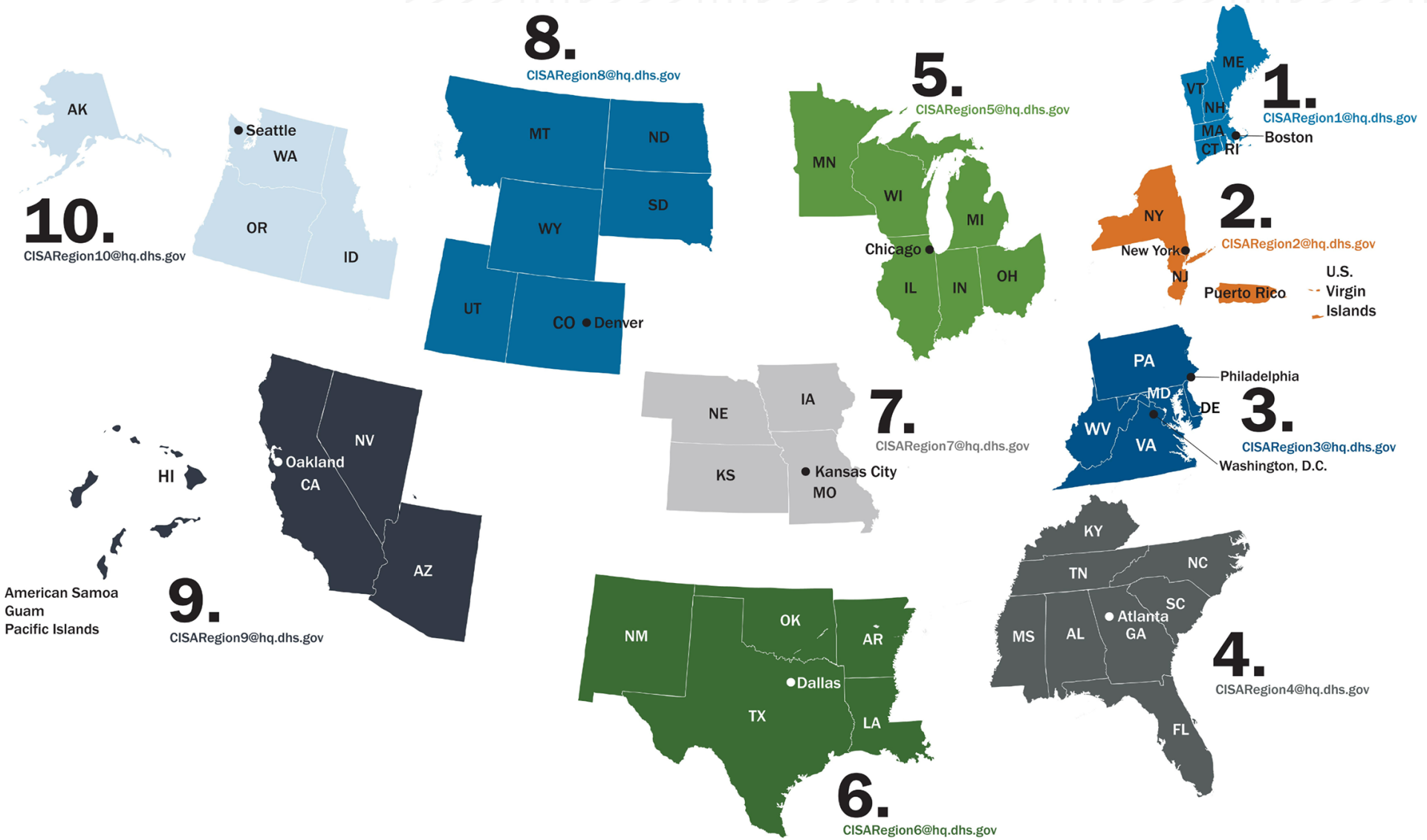
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

16 Critical Infrastructure Sectors & SRMAs

CISA Regions



1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Irving, TX
7	Kansas City, MO
8	Lakewood, CO
9	Oakland, CA
10	Seattle, WA
CS	Pensacola, FL

CISA Regional Teams

- Regional Director
- Deputy, Regional Director
- Chief, Protective Security Advisor
- **Protective Security Advisor (PSA)**
- Chief, Chemical Security Inspector
- **Chemical Security Inspector (CSI)**
- Senior Chemical Security Inspector
- Regional Operations Manager
- Critical Infrastructure Specialist
- Operations Analyst
- National Risk Management Center Regional Analyst

Gray: Regional Office
Blue: Field Personnel

- Regional Regulatory Analyst (TBA)
- Administrative Officer
- Program Analyst for Business Support (TBA)
- Outreach Coordinator
- Interagency Security Committee (ISC) Regional Advisor
- Regional Training & Exercise Coordinator
- Regional Planner (TBA)
- External Affairs Officer
- Chief, Cybersecurity Advisor
- **Cybersecurity Advisor (CSA)**
- **Emergency Communications Coordinator (ECC)**
- **Bombing Prevention Coordinator (BPC)**

October is Cybersecurity Awareness Month

Cybersecurity Awareness Month

- Launched in 2004
- Co-managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance
- Collaborative effort between government and industry to raise cybersecurity awareness
- Ensures that everyone has the resources they need to be safe and secure online.

What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Wherever there is technology, there needs to be cybersecurity

Why is it Important?

- Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.
- For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

Cyber Threats of Today

- **Ransomware (including RaaS)**
  - Volt Typhoon (e.g., command-line interface "CLI")
  - MOVEit (injection of SQL commands to access the databases)
  - ESXIArg (VMWare ESXI servers)
  - Royal (ConnectWise)
  - Darkside (Market hacking tools stealing data)
  - REvil/ Sodinokibi (targeting MSPs)

- **APTs and Nation-State Threats**
  - Killnet (Pro-Russian hackers conducting DDoS attacks)
  - APT28, APR29, APT41, etc.,
  - FIN7, FIN11, etc.

- **Other malware**
  - Remote Access Trojans (RATs): **e.g., Trickbot**, **Emotet**, LokiBot, IcedID, BazarLoader
  - wiperware: NotPetya; Acid Rain, WhisperGate, Hermetic Wiper

- **Threats to External Dependencies**
  - 3rd party vendors, service providers, infrastructure providers
  - **Supply chain attacks**: SolarWinds, Kaseya, Kronos, etc.

- **Other Threats to Financial Services**
  - Phishing, BEC, PoS breach, Insider Threat, DDoS, etc.

The Threat is Real

- Yahoo Data Breach (2017) - 3 billion accounts.
- Starwood (Marriott) Data Breach (2018) - 500 million guests.
- Facebook Data Breach (2019) - 533 million users.
- Solarwinds (2020) - 18,000 businesses were affected.
- Colonial Pipeline (2021) – 50 million users.
- Lapsus$ (2022) - 57 million customer records
- MOVEit (2023) - 200+organizations and up to 17.5 million individuals

Transportation Cyber Risks

- Social Engineering
- Hackers
- Corrupted Data
- Contingent System Failure
- Inoperable Electronic Logging Devices
- Varying State Laws
- Errors by Contractors
- Bodily Injury and Property Damage

Feelings Towards Cybersecurity

- **78%** of people consider staying secure online a priority
- **57%** of respondents expressed they were worried about cybercrime
- **46%** felt frustrated while staying secure online
- **39%** of users trying to keep safe felt information on how to stay secure online is confusing

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

Our Online Behaviors

- **Only 33% of individuals create unique passwords for all accounts**
  - Only 18% of individuals have downloaded a password manager
- **43% of respondents have never heard of multifactor authentication.**
  - Out of the 57% of the participants who had heard about it:
    - 79% applied it at least once and 94% of them reporting that they were still using MFA
- **92% of respondents took action after a security training**
  - 58% say they are better at recognizing phishing
  - 45% started using strong and unique passwords
  - 40% started using MFA
  - 40% started regularly installing software updates

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

How Safe is your Data?

Facts

SOBERING CYBER STATS

1 IN 3 HOMES
with computers are infected with
MALICIOUS SOFTWARE

65% OF AMERICANS
who went online received
at least one online scam offer.

Worldwide, consumers
LOST $358
+21 HOURS
on average per year
dealing with online crime.

47% OF AMERICAN ADULTS
have had their personal information
exposed by cyber criminals.

600,000 ACCOUNTS HACKED
every single day.

THE #1 CYBER CRIME is the
IMPOSTER SCAM
with 1 in 5 people reporting
a financial loss.

More Facts

1. Microsoft Security Intelligence Report and Consumer Reports
2. AARP, “Caught in the Scammer’s Net: Risk Factors That May Lead to Becoming an Internet Fraud Victim,” 2014
3. Norton Cyber Security Insights Report Q1, 2017
4. Ponemon Institute, “2015 Cost of Cyber Crime Study: Global,” 2015
5. Facebook
6. Federal Trade Commission, “The Top Frauds of 2017”
7. staysafeonline.org

Social Media Surveys

First Job Title:	STOP
Favorite Food:	GIVING
Favorite Color:	PEOPLE
First Pet's Name:	YOUR
First Child's Name:	PERSONAL
Favorite Restaurant:	INFORMATION
Where Are You From:	TO
Favorite Singer/Band:	GUESS
Mother's Maiden Name:	YOUR
First Type of Car:	PASSWORDS
First Job:	AND
Favorite Band:	SECURITY
High School Mascot:	QUESTIONS

What are our we seeing?

- Threat actors are performing scans for open/known vulnerabilities to exploit.
- Gaining access to privileged accounts using stolen credentials.
- Performing reconnaissance on the organization and gathering data.
- Moving laterally through the organization to eventually to extort for financial gain.
- Organization will patch to prevent the intrusion and the adversary will scan and try to attempt access again

New ERA for Product Security

Protective Measures in the “New Normal”

What your IT, and IT Security shops need to have in place (i.e., *the basics*)

Today

- Inventory all people, processes, technology and information
- Document critical systems and the services they support
- **Have a plan for responding to cyber incidents**
- **Backup all data and test backed-up data regularly**
- Deploy and update endpoint detection on all servers and workstations
- Turn on logging for all network appliances, servers and services
- **Develop and Implement comprehensive patch management process**

Tomorrow

- **Implement strong identity management practices (i.e., MFA)**
- **Plans to decommission End of Life systems**
- Develop and strengthen situational awareness
- Implement innovative security awareness training
- Implement a secure network architecture
- Conduct internal audits and periodic cyber assessments
- Utilize cyber attack frameworks when responding to cyber incidents

Protective Measures in the “New Normal”

Organizational Leaders

- **Know** business risks and treat cyber attacks as a risk area, to operations and to supply chains
- **Foster** a culture of operational resilience and cyber readiness
- **Incorporate** cybersecurity as a part of business strategy, including all external relationships
- **Build** and expand a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information, incident reporting, and response coordination

All End Users

- Participate in security awareness training and a general awareness in cyber threats
- Be aware of your digital footprint and know the end-user security features available to you
- Practice good operational security when participating in web conferencing
- Know the data backup options available and ensure locally stored data is backed up
- Be vigilant, accountable, and report incidents and suspicious activity immediately

4 Easy Ways to Stay Safe Online

Use Strong Passwords and a Password Manager

Turn on Multifactor Authentication

Recognize and Report Phishing Attacks

Update Your Software

Use Strong Passwords

CREATE STRONG PASSWORDS:

- **Long**
  - Over 16 characters
- **Unique**
  - NEVER reuse passwords
- **Complex**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks

Turn on Multifactor Authentication

WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  Fingerprint
  Facial recognition

Turn on Multifactor Authentication

WHERE SHOULD YOU USE MFA?

- **Email**
- **Accounts with financial information**
  Ex: Online store
- **Accounts with personal information**
  Ex: Social media

Recognize and Report Phishing

PHISHING RED FLAGS:

- **A tone that's urgent or makes you scared**

"Click this link immediately or your account will be closed"

- **Bad spellings, bad grammar**
- **Requests to send personal info**
- **Sender email address doesn't match the company it's coming from**

Ex: Amazon.com vs. Amaz0n.com

- **An email you weren't expecting**

Recognize and Report Phishing

WHAT TO DO

Do NOT

- Don't click any links
- Don't click any attachments
- Don't send personal info

Do

- Verify
- Contact that person directly if it's someone you know
- Report it to your IT department or email/phone provider
- DELETE IT

Update Your Software

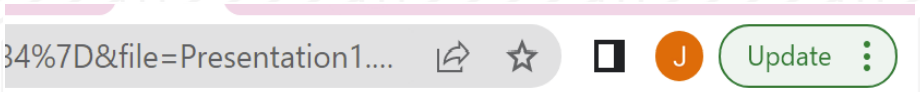
WHY?

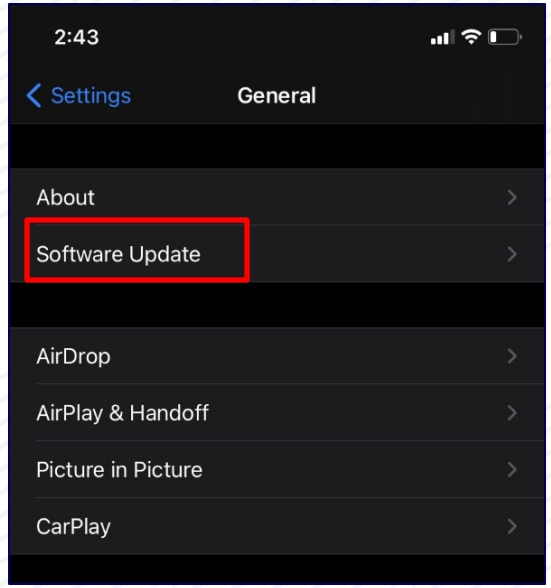
- Updates ensure your devices and apps are protected from the latest threats
- Don't click "remind me later", it could leave you vulnerable to cyber threats
- Automatic updates are the easiest way to stay secure

Update Your Software

WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts





Sampling of Voluntary & No-Cost Cybersecurity Offerings

- **Assessments & Evaluations**
  - Cross-Sector Cybersecurity Performance Goals (CPG)
  - Cyber Resilience Reviews (CRR™)
  - Cyber Infrastructure Surveys
  - ~~Phishing Campaign Assessment~~/Technical Phishing Test
  - Vulnerability Scanning & Web Application Scanning
  - Risk and Vulnerability Assessments (aka "Pen" Tests)
  - External Dependencies Management Reviews
  - Cyber Security Evaluation Tool (CSET™)
  - Validated Architecture Design Review (VADR)

- **Preparedness Activities**
  - Alert and notifications on threats, vulnerabilities, and mitigations
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Workshops (Cyber Resilience, Cyber Incident Management, Election Security, etc.)

- **Partnership Development**
  - Informational Exchanges
  - Working Group Support
  - Cyber Information Sharing and Collaboration Program (CISCP)

- **Strategic Messaging & Advisement**
  - Resource Briefings
  - Keynotes and Panels
  - Threat Briefings
  - Topic Specifics (e.g., NCSAM, SCRM, ICS, etc.)

- **Incident Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination
  - Targeted (Victim) Notifications

Sampling of Voluntary & No-Cost Cybersecurity Offerings

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org
- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs, visit www.isao.org/about.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

Maritime Transportation System Information Sharing and Analysis Center

MEISAC
MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

Real Estate ISAC Information Sharing and Analysis Center

ONG-ISAC

RETAIL & HOSPITALITY ISAC

National Defense ISAC

WATER ISAC

DNG-ISAC

SPACE ISAC

H-ISAC HEALTH - ISAC

Surface Transportation Information Sharing and Analysis Center

REN-ISAC

IT ISAC

AVIATION ISAC

FS-ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

AUTO-ISAC Automotive Information Sharing and Analysis Center

Incident Coordination & Response

Contact CISA

Report cybersecurity incidents and vulnerabilities:

888-282-0870

central@cisa.gov

Threat Hunting Services

Provides incident response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors as well as government entities at the Federal, State, Local, Tribal, and Territorial levels

Additional CISA Resources:

- **School Safety:** School Safety | Cybersecurity and Infrastructure Security Agency CISA
- **Protecting Our Future:** Protecting Our Future: Cybersecurity for K-12 | CISA
- **Goose Tool (Flexible Hunt and IR Tool):** https://www.cisa.gov/resources-tools/resources/untitled-goose-tool-fact-sheet (Click on the "Untitled Goose Tool" where you will find a lot information on Prerequisites, Requirements and installation (Scroll down and look under Table of Contents.)
- **STOP RANSOMWARE:** https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr
- **Download the CSET Tool:** https://www.cisa.gov/downloading-and-installing-cset
- **Cross-Sector Cybersecurity Performance Goals (CPG):** https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- **Cyber Resource Hub:** https://www.cisa.gov/cyber-resource-hub
- **Cyber Essentials:** https://www.cisa.gov/cyber-essentials
- **Vulnerability Disclosure Policy Template:** https://www.cisa.gov/vulnerability-disclosure-policy-template
- **CISA Incident Reporting Form:** https://us-cert.cisa.gov/forms/report
- **Cybersecurity Training and Exercises:** https://www.cisa.gov/cybersecurity-training-exercises
- **CISA Tabletop Exercise Packages:** https://www.cisa.gov/cisa-tabletop-exercises-packagesCISA
- **Cyber Incident Response : https://us-cert.cisa.gov/forms/report and/or Filing a Complaint with IC3:** https://www.ic3.gov/

Rahul Mittal

Cybersecurity Advisor, Region 3
National Capitol Region
Rahul.mittal@cisa.dhs.gov

Regional Support:
CISARegion3@hq.dhs.gov

To Report an Incident:
https://us-cert.cisa.gov/report

To Report a Criminal matter:
https://www.ic3.gov/

Media Inquiries:
CISAMedia@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Q&A and Closing Remarks

Jeremy Furrer
Safety Policy and Promotion Division Chief
Office of Transit Safety and Oversight

Q&A

Thank you!

https://www.transit.dot.gov/TSOWebinars

TRANSIT.DOT.GOV