Cybersecurity Awareness for Transit Agencies Webinar

November 3, 2022

Office of Transit Safety and Oversight

Federal Transit Administration

U.S. Department of Transportation
Federal Transit Administration

Introduction

Angela Dluger

Deputy Associate Administrator,

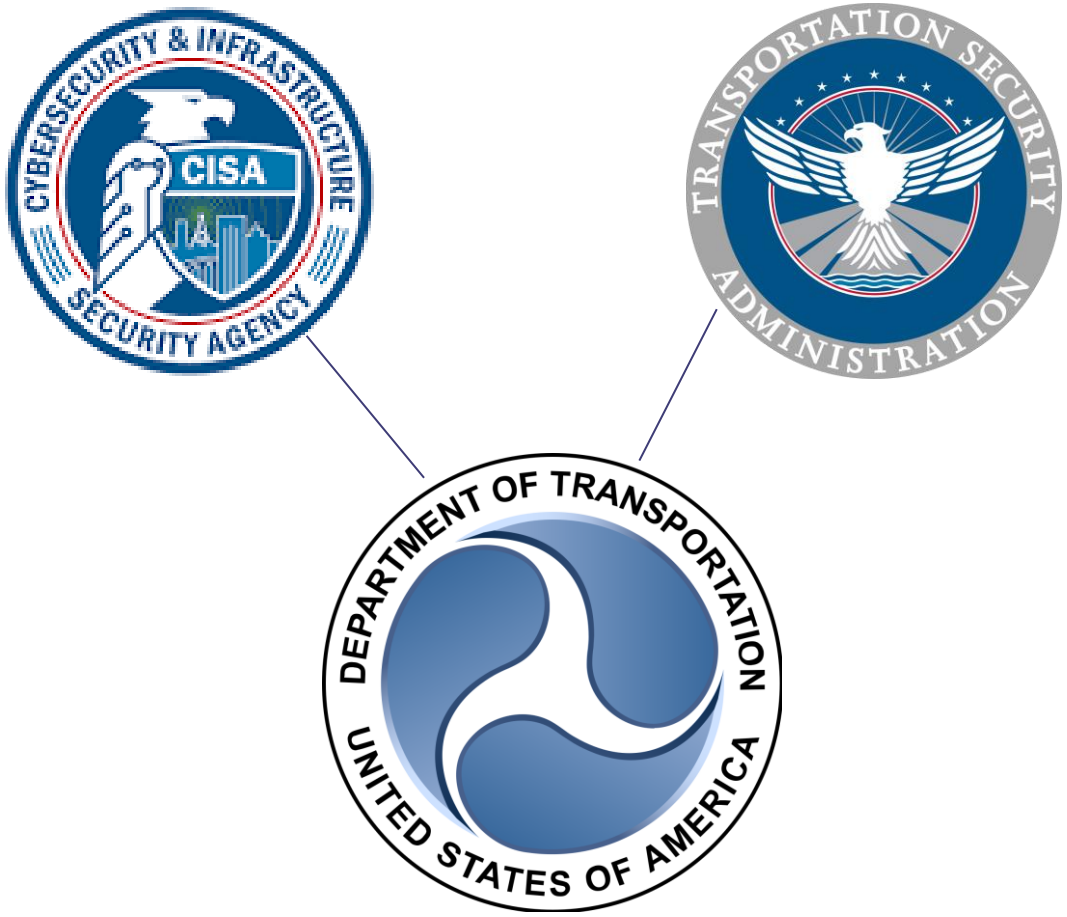
Office of Transit Safety and Oversight

Federal Transit Administration

Cybersecurity Threats to the Transit Industry

- The threat of cyber disruption to critical infrastructure is at an all-time high
- Increasing attacks demonstrate the ability of unauthorized users to access sensitive information and impact critical infrastructure systems

Federal Coordination on Cybersecurity



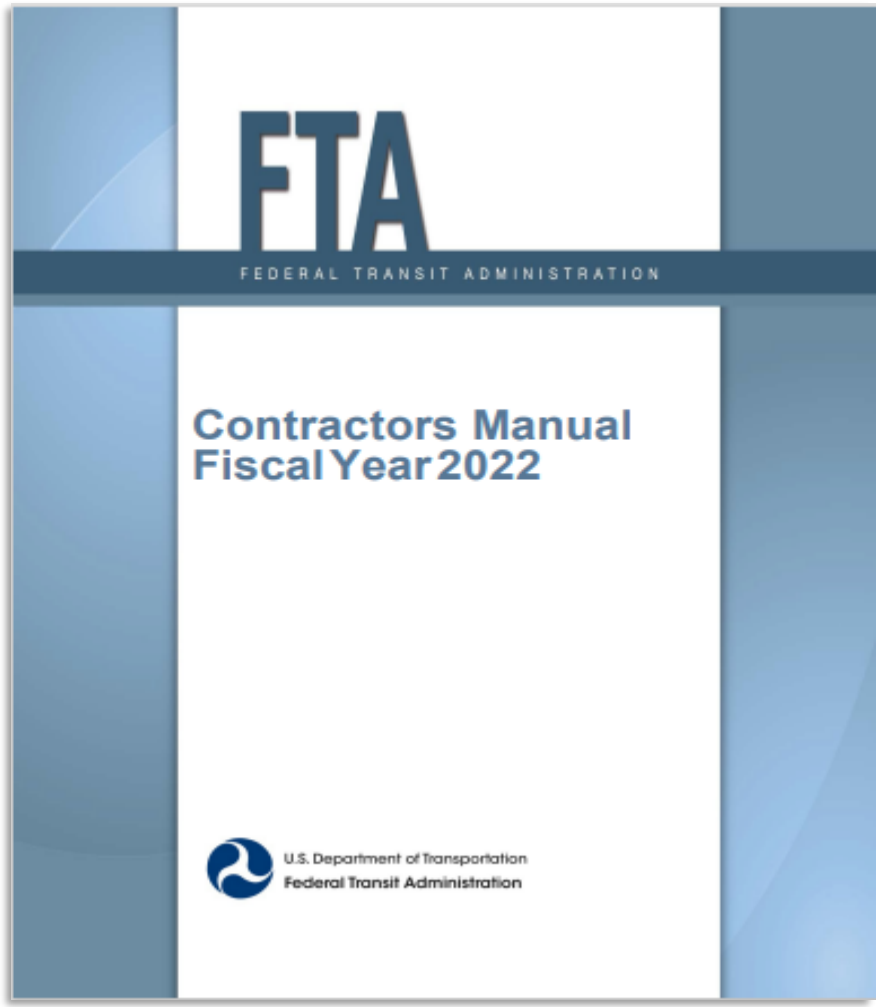
Cybersecurity: DHS Requirements

- Security Directive (SD) 1582-21-01A
  - Applies to the rail entities affected by TSA's Security Training rule
- Information Circular
  - *Non-regulatory like the Security Directive*
- Originally Issued December 31, 2021
- SD Extended on October 24, 2022

- Four actions for passenger and transit rail:
  - Cybersecurity Coordinators
  - Reporting to CISA
  - Incident Response Plan
  - Vulnerability Assessment

Cybersecurity Review Area for FTA's Triennial Review

- In Fiscal Year (FY) 2022, FTA added the Cybersecurity Section as a review area to the Triennial Review Contractors Manual.
- Review is to ensure that recipients certified in the Transit Award Management System (TrAMS) develop, maintain and execute a written plan for identifying and reducing Cybersecurity risks.



Eligible Cybersecurity Expenses

While cybersecurity costs are not directly addressed in FTA's authorizing legislation, they are allowable under various FTA programs in areas such as:

- **Operating Assistance**
- **Crime Prevention and Security Projects**
- **State of Good Repair**

Any costs associated with an award, including cybersecurity costs must be:

- Allowable, Reasonable, and Allocable

Funding Requirements for 5307 Transit Agencies

1% Security Funding required for 5307 Transit Agencies

Fiscal Year	Number of 5307 Awarded Recipients that Selected Yes to 1% Security Question	Number of 5307 Awarded Recipients	Percent of 5307 Awarded Recipients
2015	268	557	48%
2016	340	688	49%
2017	419	778	54%
2018	427	774	55%
2019	432	754	57%
2020	475	762	62%

FTA's Cybersecurity Resources

Cybersecurity Resources for Transit Agencies

https://bit.ly/3AQQWqe

Contact

Angela Dluger
Deputy Associate Administrator for Transit Safety and Oversight
Federal Transit Administration
angela.dluger@dot.gov

TRANSIT.DOT.GOV

SEE YOURSELF IN CYBER

CYBERSECURITY AWARENESS MONTH 2022

Rahul Mittal
Cybersecurity Advisor for Washington D.C. Region III
(MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Awareness Month Theme

The 2022 Campaign theme, See Yourself in Cyber, emphasizes that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October, we will focus on the "people" part of cybersecurity, providing information and resources to help Americans make smart decisions on the job, at home, at school, and in the future.

In Partnership:
StaySafeOnline.org

CYBERSECURITY AWARENESS MONTH 2022

Partnership

The Cybersecurity and Infrastructure Security Agency (CISA) is the federal lead for Cybersecurity Awareness Month with the National Cybersecurity Alliance (NCA) as co-lead.

National Cybersecurity Alliance (staysafeonline.org)

CYBERSECURITY AWARENESS MONTH 2022

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.

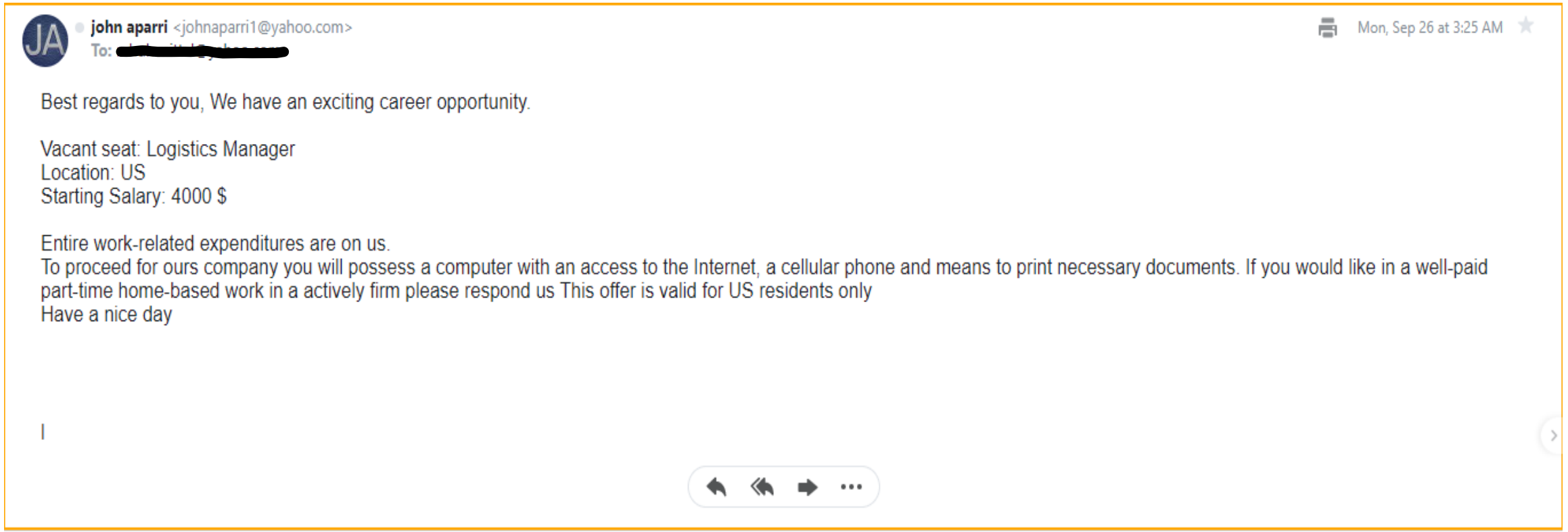
CYBERSECURITY AWARENESS MONTH 2022

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

CYBERSECURITY AWARENESS MONTH 2022

Example of Phishing



john aparri <johnaparri1@yahoo.com>
To: [redacted]

Mon, Sep 26 at 3:25 AM

Best regards to you, We have an exciting career opportunity.

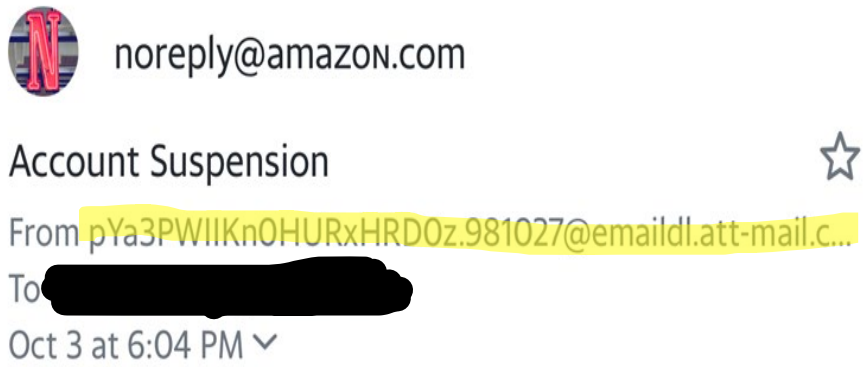
Vacant seat: Logistics Manager
Location: US
Starting Salary: 4000 $

Entire work-related expenditures are on us.
To proceed for ours company you will possess a computer with an access to the Internet, a cellular phone and means to print necessary documents. If you would like in a well-paid part-time home-based work in a actively firm please respond us This offer is valid for US residents only
Have a nice day

I

CYBERSECURITY AWARENESS MONTH 2022

Another Example of Phishing



amazon

Hello,

We have temporarily placed your Amazon account on hold and canceled any pending orders or subscriptions because we detec ted unusual activity on it.

To restore your account, you can click the button below and follo w on-screen instructions. Once you have provided the required information, we will review it and respond within 24 hours.

You cannot access your account until this process is complete.

If you don't complete account recovery within 3 days, we will lock your amazon account permanently.

Sincerely,

Customer Service
Amazon.com

Sign-in to Amazon

CYBERSECURITY AWARENESS MONTH 2022

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

CYBERSECURITY AWARENESS MONTH 2022

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

https://www.cisa.gov/stopransomware/resources

CYBERSECURITY AWARENESS MONTH 2022

Action Steps

This year's campaign goal is to have everyone implement these four action steps to increase online security:

- **Enable Multi-Factor Authentication**: You need more than a password to protect your online accounts, and enabling MFA makes it 99% less likely you will get hacked
- **Use Strong Passwords**: Use passwords that are long, unique, and randomly generated.
- **Recognize and Report Phishing**: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software**: Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.

CYBERSECURITY AWARENESS MONTH 2022

Enable Multi-Factor Authentication

- If you can do just one thing to protect your online valuables, set up Multi-factor Authentication.
- It goes by many names: Two Factor Authentication. Multifactor Authentication. Two Step Factor Authentication. MFA. 2FA. They all mean the same thing: opting-into an extra step when trusted websites and applications ask you to confirm you're really who you say you are.
  - Visit CISA's Multi-Factor Authentication resources for more information
    - https://www.cisa.gov/mfa

CYBERSECURITY AWARENESS MONTH 2022

Multi-Factor Authentication

- Type 1: Something Only the User Knows
  - Password
  - Pattern
  - Picture
  - PIN
- Type 2: Something only the user holds
  - Token
  - Public Key Token
- Type 3: Something only the user is or does
  - Morphological Biometrics
  - Behavior Biometrics

Use Strong Passwords

- Creating strong passwords is an easy way to improve your cybersecurity. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Be sure to use different passwords for different accounts.
- Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- Put cybersecurity first by protecting the information stored on devices. Much of a user's personal information is stored either on their computer, smartphone, tablet or possibly someone else's system.

Password Managers

- One password to rule them all.
- Generates random passwords which makes it harder to guess.
- Simple access to multiple accounts.
- Can be used over multiple devices.
- Passwords are encrypted from malicious activity.

Recognize and Report Phishing

- Have you ever seen a link that looks a little off? It looks like something you've seen before, but it says you need to change or enter a password. Or maybe it asks you to verify personal information.
- It's likely a phishing scheme: a link or webpage that looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites.

Don’t Wait -Update your software

- Bad actors are always looking for software flaws to exploit and network defenders work diligently to find and fix them before it happens.
- But our network defenders can’t do it alone. They rely on all of us to do our part as well.
- So, turn on automatic updates for all your devices, keep your systems and software up-to-date and updates are available, don’t procrastinate. Take a moment and make the update.

Things We Can

- Creating strong passwords is an easy way to improve your cybersecurity. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Be sure to use different passwords for different accounts.
- Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- Put cybersecurity first by protecting the information stored on devices. Much of a user's personal information is stored either on their computer, smartphone, tablet or possibly someone else's system.

Transportation Sector Security

- CISA non-regulatory and TSA determine the requirements for this sector.
- TSA Surface Transportation Cybersecurity Toolkit https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit
- Autonomous Ground Vehicles Security Guide http://www.cisa.gov/publication/autonomous-ground-vehicle-security-guide-transportation-systems-sector
- Modern Vehicle Cybersecurity from NHTSA https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
  - https://www.cisa.gov/circia

Resources

- NIST Risk Management Framework SP 800-37 Rev 2
  https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- NIST 800-53 Rev 5 (Control Catalog)
  https://csrc.nist.gov/projects/risk-management
- Cloud Security Technical Reference Architecture
  https://www.cisa.gov/cloud-security-technical-reference-architecture
- State and Local Cybersecurity Grant Program
  https://www.cisa.gov/cybergrants
- Cybersecurity and Physical Security Convergence Action Guide
  cisa.gov/publication/cybersecurity-and-physical-security-convergence
- Insider Threat Mitigation
  cisa.gov/insider-threat-mitigation
- Cyber Resource Hub
  cisa.gov/cyber-resource-hub
- Cyber Hygiene Services
  cisa.gov/cyber-hygiene-services
- Cybersecurity Advisors
  cisa.gov/csa
- Protective Security Advisors
  cisa.gov/protective-security-advisors
- CISA Tabletop Exercises Packages
  cisa.gov/cisa-tabletop-exercises-packages
- For more information or to seek additional help, contact us at
  Central@cisa.gov

CYBERSECURITY AWARENESS MONTH 2022

Website and Resources

For complete information and resources on Cybersecurity Awareness Month, go to: **www.cisa.gov/cybersecurity-awareness-month**

SHIELDS UP

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
    - Cyber Hygiene Services
    - Risk and Resilience-based Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis
- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Workshops
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

Report a Cyber Issue

- CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

www.cisa.gov/report

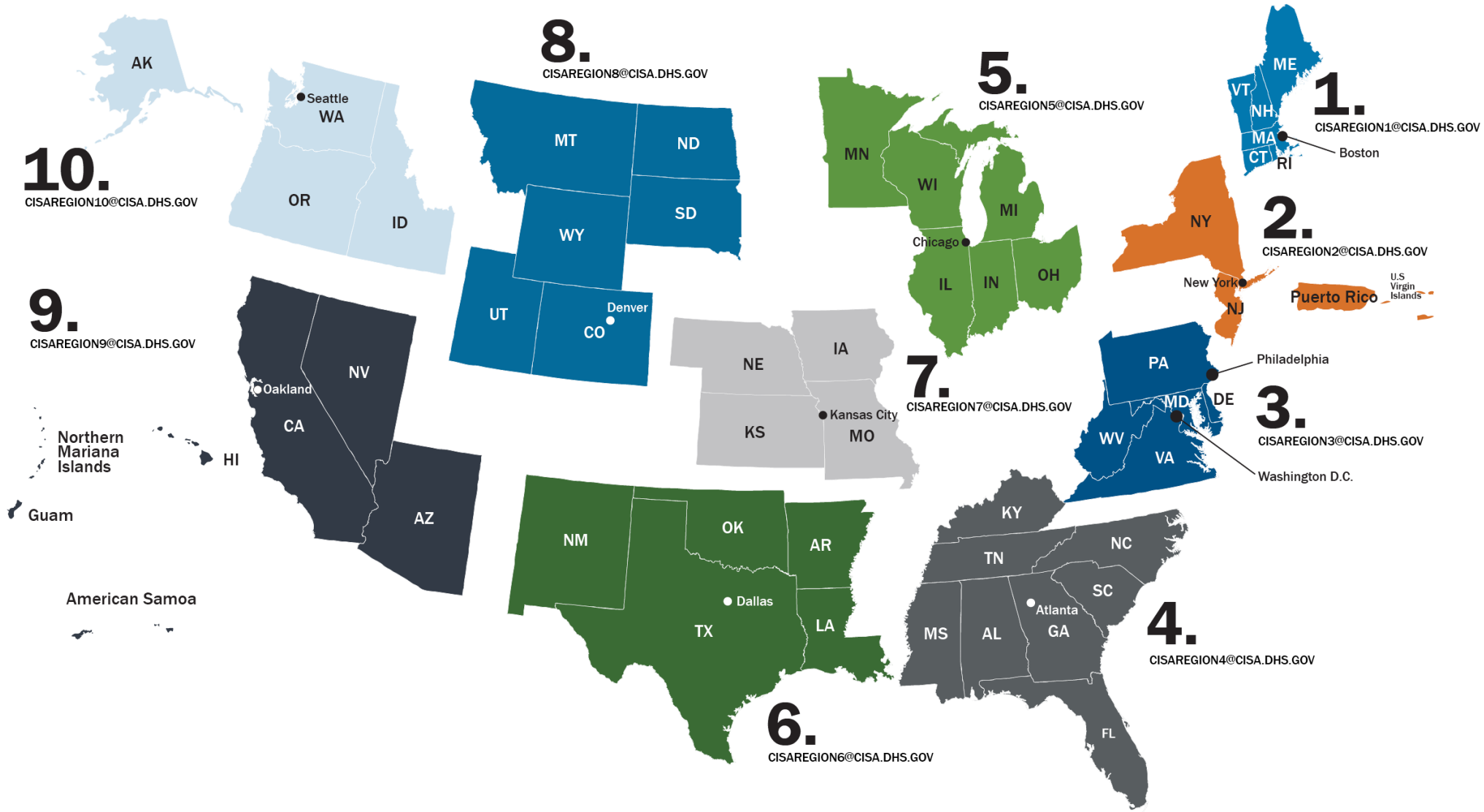
- If you have experienced an actual incident that requires a criminal investigation, contact FBI 24x7 CyWatch: (855) 292-3937 or

CyWatch@fbi.gov

CYBERSECURITY AWARENESS MONTH 2022

CISA Regions

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



CISA Contact Information

Rahul Mittal, CSA for Washington D.C. CISA, CISM, CRISC, CEH, CNDA	Rahul.Mittal@cisa.dhs.gov
General CISA Inquiries	central@cisa.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	Call 1-888-282-0870 Email *report@cisa.gov* visit *https://www.cisa.gov*

Website

For complete information and resources on Cybersecurity Awareness Month, go to:

www.cisa.gov/cybersecurity-awareness-month

CYBERSECURITY AWARENESS MONTH 2022


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CYBERSECURITY AWARENESS MONTH 2022


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA