Cybersecurity

★ ★ ★ ★ ★ ★

TSA Surface
FTA Joint SSO and
RTA Workshop

Transportation
Security
Administration

TSA and PPE Surface Cybersecurity – Mission and Priorities

TSA is the Transportation Systems Sector Co-Sector Specific Agency (co-SSA) with the Department of Transportation and the United States Coast Guard

TSA Mission

- Protect the nation's transportation systems to ensure freedom of movement for people and commerce

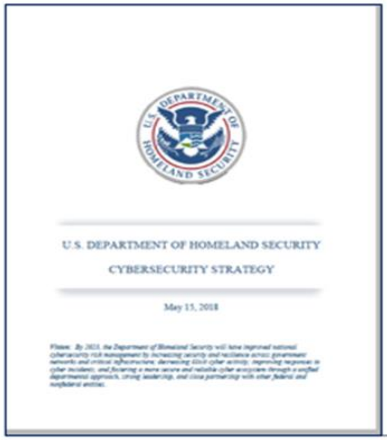
TSA Cybersecurity Priorities

- Identify cyber security risks
- Reduce vulnerabilities to our systems and critical infrastructure across the transportation systems sector
- Mitigate consequences if and when incidents do occur
- Strengthen security and ensure the resilience of the Transportation system

Surface Cybersecurity Priorities

- Cyber Critical Infrastructure Protection
- Cybersecurity Awareness and Outreach
- Information Sharing and Working Groups
- Managing Risks through Industry Engagement

Cybersecurity Mandates



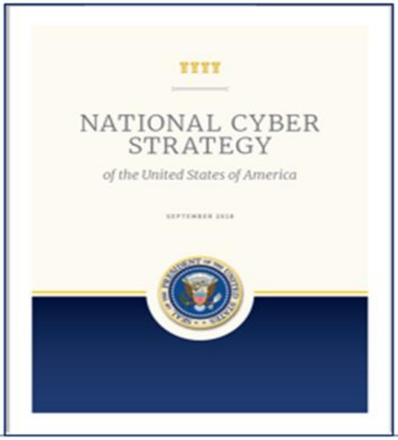
U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY STRATEGY

May 15, 2018

Vision: By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.

Released May 2018

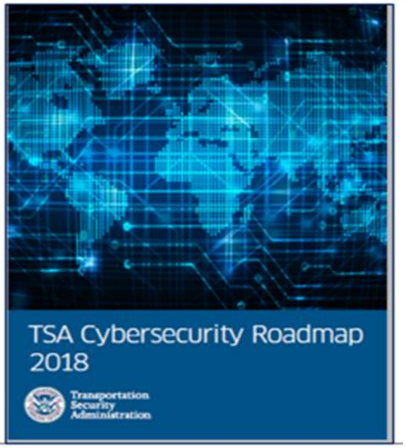


NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018

Released September 2018



TSA Cybersecurity Roadmap 2018

Transportation Security Administration

Released November 2018

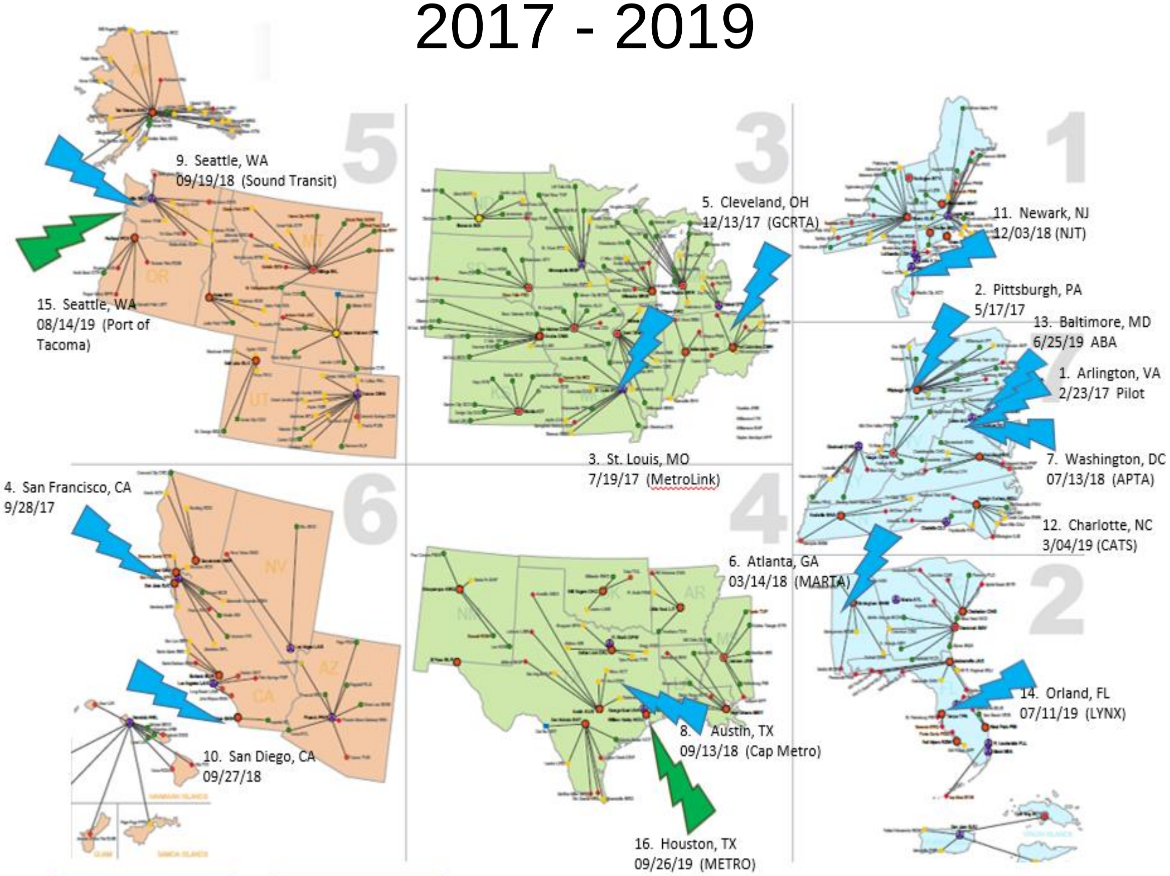
TSA Cybersecurity Roadmap identifies four major priorities that will help the agency achieve its cybersecurity goals:

- Identify cyber security risks
- Reduce vulnerabilities to our systems and critical infrastructure across the transportation systems sector
- Mitigate consequences if and when incidents do occur
- Strengthen security and ensure the resilience of the Transportation system

Transportation
Security
Administration

Surface Cybersecurity – Workshops

2017 - 2019



1. Arlington, VA 2/23/17 Pilot

2. Pittsburgh, PA 5/17/17

3. St. Louis, MO 7/19/17 (MetroLink)

4. San Francisco, CA 9/28/17

5. Cleveland, OH 12/13/17 (GCRTA)

6. Atlanta, GA 03/14/18 (MARTA)

7. Washington, DC 07/13/18 (APTA)

8. Austin, TX 09/13/18 (Cap Metro)

9. Seattle, WA 09/19/18 (Sound Transit)

10. San Diego, CA 09/27/18

11. Newark, NJ 12/03/18 (NJT)

12. Charlotte, NC 3/04/19 (CATS)

13. Baltimore, MD 6/25/19 ABA

14. Orland, FL 07/11/19 (LYNX)

15. Seattle, WA 08/14/19 (Port of Tacoma)

16. Houston, TX 09/26/19 (METRO)

COMPLETED PLANNED

As of July 11, 2019, TSA Surface through the Intermodal Security Training and Exercise Program (I-STEP) has conducted 14 Cybersecurity Workshops

Transportation
Security
Administration

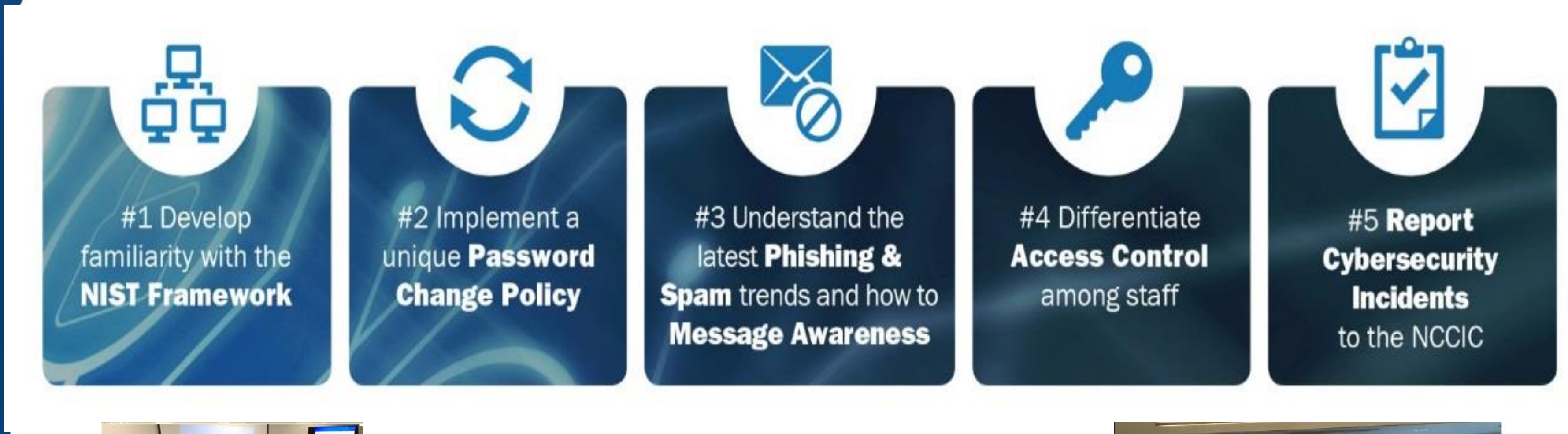
Surface Cybersecurity Workshops

Multi-modal participants receive five nontechnical takeaways to consider over five days (“5N5”) to enhance their transportation organizations’ cybersecurity posture

Workshop Goals

1. Inform stakeholders (industry and federal) about cybersecurity “No Cost” resources and programs to elicit feedback
2. Facilitate discussion of best practices and lessons learned associated with implementing cybersecurity measures
3. Provide multi-modal participants with five nontechnical actions to consider over five days (“5N5”) to enhance their transportation organizations’ cybersecurity posture

5N5 Nontechnical Cybersecurity Actions



#1 Develop familiarity with the **NIST Framework**

#2 Implement a unique **Password Change Policy**

#3 Understand the latest **Phishing & Spam** trends and how to **Message Awareness**

#4 Differentiate **Access Control** among staff

#5 **Report Cybersecurity Incidents** to the NCCIC

Transportation
Security
Administration

DHS CISA Cybersecurity Role

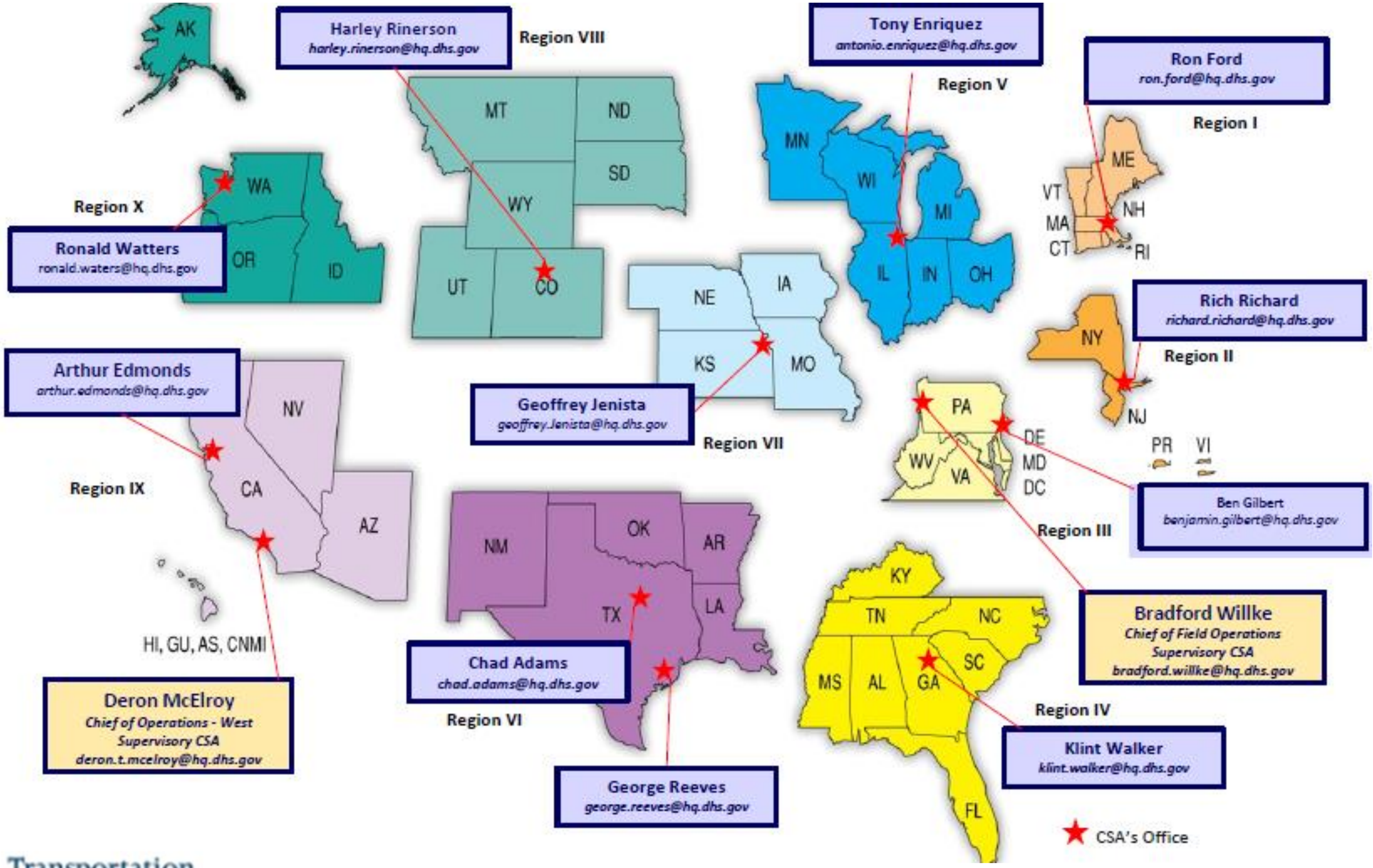
CISA
CYBER+INFRASTRUCTURE

- **Cybersecurity & Infrastructure Security Agency (CISA)**
  Leads Federal cybersecurity programs

- **Cyber Security Division**
  Leads efforts to enhance the security of cyber and communications infrastructure
  - Information sharing
  - Risk assessments
  - Technical assistance
  - Education
  - Incident response

CISA provides more than 40 cybersecurity tools and resources for public and private sector stakeholders

Cybersecurity Advisors



Harley Rinerson
harley.rinerson@hq.dhs.gov

Tony Enriquez
antonio.enriquez@hq.dhs.gov

Ron Ford
ron.ford@hq.dhs.gov

Ronald Watters
ronald.waters@hq.dhs.gov

Rich Richard
richard.richard@hq.dhs.gov

Arthur Edmonds
arthur.edmonds@hq.dhs.gov

Geoffrey Jenista
geoffrey.Jenista@hq.dhs.gov

Ben Gilbert
benjamin.gilbert@hq.dhs.gov

Bradford Willke
Chief of Field Operations
Supervisory CSA
bradford.willke@hq.dhs.gov

Chad Adams
chad.adams@hq.dhs.gov

Deron McElroy
Chief of Operations - West
Supervisory CSA
deron.t.mcelroy@hq.dhs.gov

Klint Walker
klint.walker@hq.dhs.gov

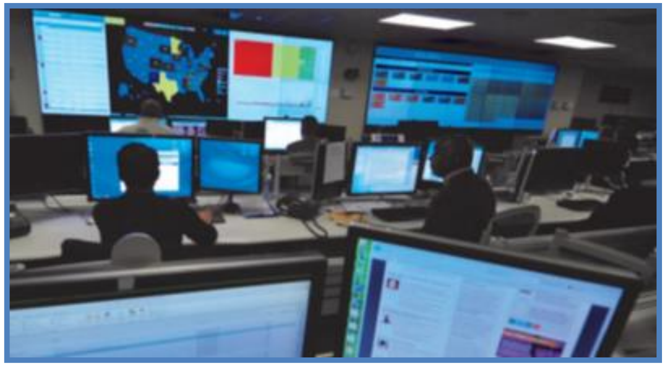
George Reeves
george.reeves@hq.dhs.gov

★ CSA's Office

DHS NCCIC

National Cybersecurity Communications and Integration Center (NCCIC)

- Manages 24/7 cybersecurity operations center
- Provides cybersecurity scanning, testing, threat analysis, mitigation, and incident management services
- Coordinates cyber activities with law enforcement, intelligence, and defense communities



Alerts, Bulletins, Security Updates, Best Practices

US-CERT

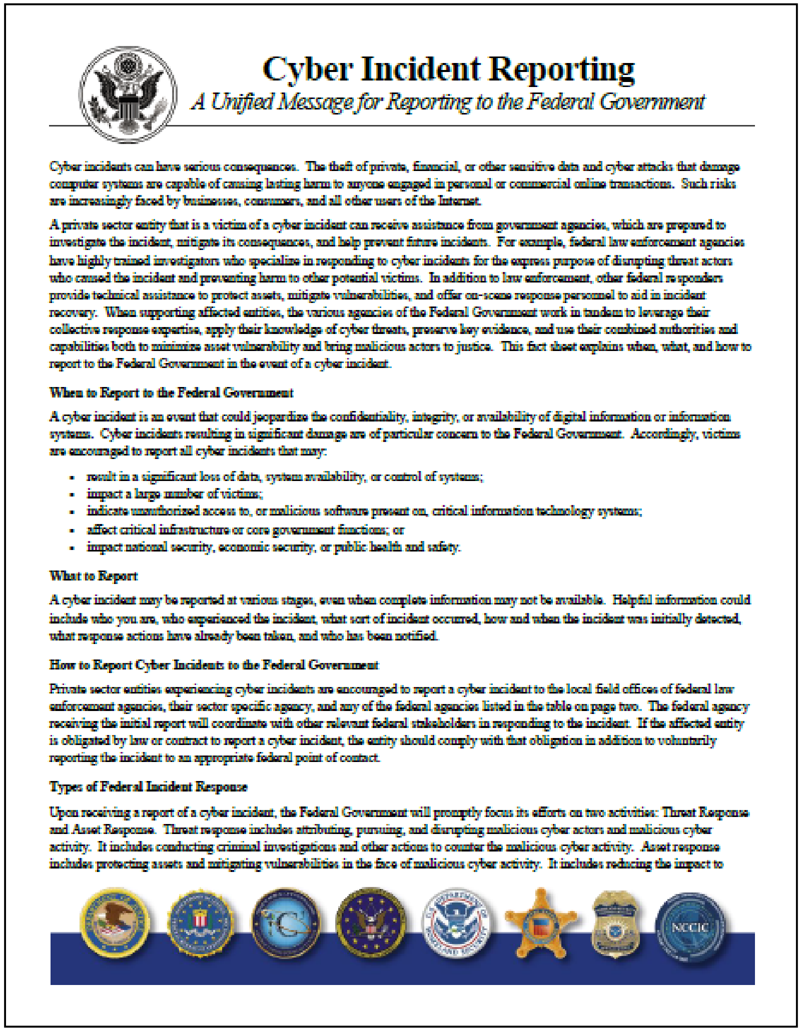
https://www.us-cert.gov/

ICS-CERT

https://ics-cert.us-cert.gov/

Transportation Security Administration

Incident Reporting



Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

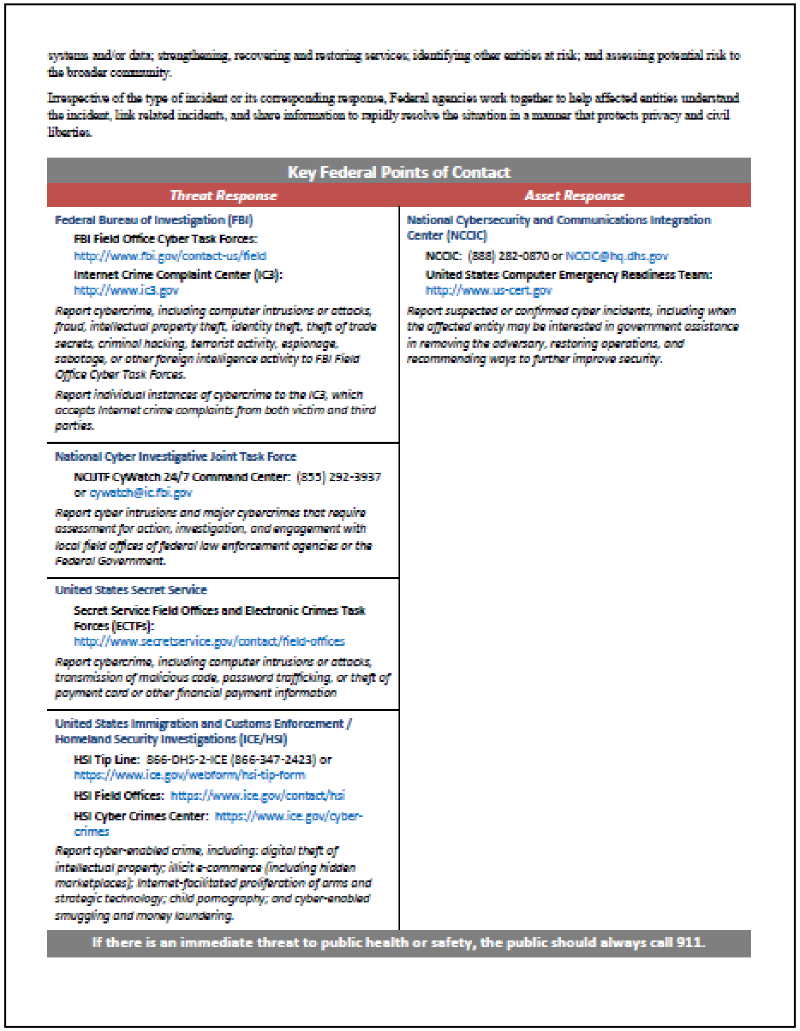
A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to



systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

Threat Response	*Asset Response*
Federal Bureau of Investigation (FBI) **FBI Field Office Cyber Task Forces:** http://www.fbi.gov/contact-us/field **Internet Crime Complaint Center (IC3):** http://www.ic3.gov *Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.* *Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.*	National Cybersecurity and Communications Integration Center (NCCIC) **NCCIC:** (888) 282-0870 or NCCIC@hq.dhs.gov **United States Computer Emergency Readiness Team:** http://www.us-cert.gov *Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.*
National Cyber Investigative Joint Task Force **NCIJTF CyWatch 24/7 Command Center:** (855) 292-3937 or cywatch@ic.fbi.gov *Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.*	
United States Secret Service **Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):** http://www.secretservice.gov/contact/field-offices *Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information*	
United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) **HSI Tip Line:** 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form **HSI Field Offices:** https://www.ice.gov/contact/hsi **HSI Cyber Crimes Center:** https://www.ice.gov/cyber-crimes *Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.*	

If there is an immediate threat to public health or safety, the public should always call 911.

Incident Reporting (Continued)

When to report suspected or confirmed cyber incidents

- Potential significant loss of data, system availability, or system control
- Impact to critical infrastructure or core government function
- Indication of unauthorized access to, or malicious software present on, critical information technology systems

How to report

- NCCIC: NCCICCustomerService@hq.dhs.gov or 888-282-0870
- FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
- Transportation Security Operations Center: 866-615-5150 (Covered entities under 49 CFR Part 1580.105 and 49 CFR 1580.203)

Transportation
Security
Administration

Contact Information

Lee Allen, Surface Division Cybersecurity Lead
Lee.Allen@tsa.dhs.gov, 571-227-1251

For additional information about joining the Transportation Systems Sector Cyber Working Group or to receive This Week in Transportation Cybersecurity, email: Cybersecurity@tsa.dhs.gov

If you believe you have been a victim of a cybersecurity incident, report it to the National Cybersecurity and Communications Integration Center (NCCIC) at (888) 282-0870 or NCCICCUSTOMERSERVICE@hq.dhs.gov or to your local FBI field office

Transportation
Security
Administration