



Northern Virginia Transportation Authority

The Authority for Transportation in Northern Virginia

TRANSPORTATION TECHNOLOGY COMMITTEE

Wednesday, September 27, 2023

8:30 AM

(In-person and livestreamed via [YouTube](#))

AGENDA

- I. **Call to Order/Welcome** Councilmember David Snyder,
Chair

Action

- II. **Summary Notes of November 30th, 2022 Meeting** Councilmember David Snyder,
Chair
Recommended action: Approve meeting notes

Discussion/Information

- III. **Cybersecurity** FBI/CISA
- IV. **NVTA InNoVation Initiatives Poster** Keith Jasper, Principal,
Transportation Planning and
Programming
- V. **Transportation Technology Strategic Plan (TTSP) – Recap of First Substantive Update** Keith Jasper, Principal,
Transportation Planning and
Programming
- VI. **Artificial Intelligence in Transportation** Keith Jasper, Principal,
Transportation Planning and
Programming
- VII. **NVTA Updates** Monica Backmon, CEO
- VIII. **Member Updates**

Adjournment

- VIII. **Adjourn**

Next Meeting
TBD



Northern Virginia Transportation Authority

The Authority for Transportation in Northern Virginia

TRANSPORTATION TECHNOLOGY COMMITTEE

Wednesday, November 30, 2022, 8:30 am

Electronic meeting and livestreamed on [YouTube](#)

MEETING SUMMARY

I. Call to Order/Welcome

- Chairman Snyder called the meeting to order at 8:30 am.
- Attendees:
 - **TTC Members:** Councilmember/Chairman David Snyder (City of Falls Church and Authority Member); Mayor Jeanette Rishell (City of Manassas Park and Authority Member); Dr. Richard (Dick) Mudge (Compass); Mike Garcia (FCDOT); Andrew Meese (Transportation Planning Board); Dr. Robert Schneider (Potomac and Rappahannock Transportation Commission); Reginald Viray (Virginia Tech Transportation Institute); Brad Stertz (Audi and PAVE); Mike Fontaine (Virginia Transportation Research Council); and Jim Kolb (Summit Strategies Government Affairs).
 - **NVTA Staff:** Monica Backmon (Chief Executive Officer); Keith Jasper (Transportation Planning and Programming Principal); Dr. Sree Nampoothiri (Senior Transportation Planner) and Mackenzie Love (Regional Transportation Planner).

Action

II. Summary Notes of July 6th, 2022, Meeting

The meeting summary was approved unanimously, with abstention from members not present.

Discussion/Information

III. Transportation Technology Committee (TTC) Membership Update

Due to several members of the TTC no longer being able to participate, this was the first committee meeting for four new members. For that reason, Mackenzie Love described the goals and brief history of the TTC and the Transportation Technology Strategic Plan (TTSP) along with its ongoing updates.

The following new members were introduced to the TTC:

- Brad Stertz – Audi and PAVE (Partners for Automated Vehicle Education)
- Chris Bast – Electrification Coalition
- Supervisor Waltor Alcorn – Fairfax County Board of Supervisors
- Mike Fontaine – Virginia Transportation Research Council

The history of the TTSP which included the following highlights over the past several years was shared:

- 2017: An update to TransAction was adopted, which contained the genesis of the TTC
- 2019: First meeting of the TTC
- 2020: Draft TTSP shared with TTC
- 2021: The Authority adopted the inaugural TTSP and Action Plan
- 2022: The TTC and Authority unanimously voted to endorse expansion of the scope of strategies 4 and 8, and to add a 9th strategy

Progress updates on TTSP implementation which included ongoing coordination with Virginia Department of Transportation (VDOT) Signal Operations group from NVTA staff was shared by Mackenzie Love. Next, the Federal Highway Administration (FHWA) is developing a framework for integrating Emerging Trends and Technologies (ETTs) into Transportation Systems Management and Operations (TSMO) efforts. Lastly, there was an announcement on the status of the new InNoVation Lunch and Learn series hosted by NVTA designed to provide opportunities to exchange pragmatic information that practitioners could find useful.

- October 20th, 2022 at 11am
 - Speaker: John Zarbo, Operations Section Chief, FCDOT
 - Topic: Lessons Learned from the Relay Shuttle in Merrifield
- November 17th, 2022 at 11am
 - Speaker: Joe Stainsby, Chief Development Officer, OmniRide
 - Topic: Lessons Learned in Preparing for the Launch of Microtransit
- December 15th, 2022 at 11am
 - Speaker: Alvaro Villagran, Director of Federal Programs, Shared Use Mobility Center
 - Topic: Best Practices for Mobility Hubs

Mayor Rishell pointed out that on the TTSP Technology Timeline under 2022 – Greenhouse Gas Inventory from Department of Environmental Quality (DEQ), there should be a call out for “cold fusion” as it is another source that could help reduce greenhouse gas emissions.

IV. **Transportation Technology Strategic Plan (TTSP) Progress Update**

Mackenzie Love shared that TTSP updates were approved by the Authority on November 10th, 2022. These updates included:

- Expansion of existing strategy #4, which originally focused on minimizing Zero Occupancy passenger Vehicles, and will now also address ways to maximize potential benefits of connected and Automated Vehicles.
 - The title of strategy #4 will be changed to “Enhance operations of the multimodal transportation system through connectivity and automation.”
- Expansion of existing strategy #8 which aims to advance decarbonization of the transportation system to include new technologies that could reduce Greenhouse Gas Emissions (GHGs), such as Hydrogen, and technologies that could help improve resiliency, like Vehicle to Grid (V2G).

- Addition of a 9th strategy titled “Enhanced mobility in the region through innovation and emerging technologies in transit.”

Input on potential topics for the 8th Annual Northern Virginia Transportation Roundtable was discussed. Brad Stertz offered that hydrogen is far behind electrification and should be held off being presented. He stated that Cellular Vehicle to Everything (CV-2X) has built momentum recently and could serve as a topic for the Roundtable. Michael Fontaine mentioned smart intersection technology that looks at lidar detection of pedestrians and cyclists to track their trajectories to make intersections safer for all users. VDOT is also deploying statewide automated traffic signal performance measures, which provides a more granular perspective of the performance of traffic signals.

V. **TransAction Update**

Mr. Jasper reviewed the purpose of TransAction (TA), Northern Virginia’s long-range transportation plan through horizon year 2045, updated every 5 years, which will hopefully be the point of adoption at NVTAs December meeting. Projects in TA are evaluated as a group, not individually, and use 10 weighted performance measures. The plan includes projects that are fiscally and geographically unconstrained, with the intent to show the region’s transportation needs without any cost or geographical constraints. TA is not a funding document and does not commit NVTAs to funding any project (NVTAs Six Year program [SYP] selects projects for funding using Regional Revenues— or 70%).

With NVTAs December meeting approaching, there is anticipation of adoption of TA after about three years of development. More information regarding TA is available at <https://nvtatransaction.org/resources/>. The final plan will be uploaded to the site when it is completed.

From a technology standpoint, there are 17 of 424 projects listed in TA that are primarily technology based. These projects vary in cost and include Intelligent Transportation Systems (ITS), transit signal priority (TSP), and Electric Vehicle (EV) infrastructure projects which would be important for decarbonization.

VI. **NVTA Update**

Mr. Jasper informed the committee that the anticipated adoption of TransAction (TA) Update will retire the previous version of the plan. The newly adopted TA will be used for project eligibility for funding during the upcoming SYP application period of May 1 through July 28 of 2023, as well as the FY2026-2031 and FY2028-2033 SYPs.

VII. **Member Updates**

One TTC member also provided an update:

- Dick Mudge gave a lecture to a transportation class at George Mason focused on the macro view of automated vehicles compared with other broad-based

technologies. He went on to share that his work with Robotic Research on autonomous buses has actually looked to Advanced Driver Assistance Systems (ADAS) rather than fully automated driving. ADAS includes features like lane tracking, platooning, and collision avoidance and is more cost effective and less challenging to implement than fully automated vehicle technology. Therefore, there is a stronger focus now on ADAS. He mentioned his preference for automated Bus Rapid Transit (BRT) to be included in the next TransAction Update. He followed up by stating that the federal procurement process lacks inclusion of innovative technology, so there is an opportunity for Public-Private Partnerships (PPPs) as a way to obtain private funding to speed the process for tech-based projects. Lastly, he highlighted AV technology within freight transportation and suggested that the next TransAction update include freight technology aspects.

Adjournment

- The meeting adjourned at approximately 9:44 am.

Transportation Technology Committee Meeting

September 27, 2023

Keith Jasper
Principal, Transportation Planning and Programming





Item III: Cybersecurity



Cybersecurity in the TTSP

Strategy #3: *"Maximize Cybersecurity and Privacy for Members of the Public"*

Discussion of Cybersecurity

• Relevance to NVTA's vision and Core Values

- Transportation technology offers the potential to support NVTA's vision and enhance its mobility, accessibility, and resiliency goals, especially when deployed at scale, by enabling informed travel decisions in near real time.
- Cybersecurity strongly aligns with NVTA's Core Values of Equity, Safety, and Sustainability.

• What keeps us up at night

- The transfer of high volumes of data (infrastructure, vehicles, devices, personal) between multiple entities using information and communication technologies creates potential vulnerabilities.
- State of practice is rightly focused on minimizing vulnerabilities, but does this inhibit transportation technologies from reaching their full potential?

• NVTA's roles

- Since NVTA does not currently deploy or operate the transportation technology projects it helps to fund, initial focus has been observing state of the practice.
- Proactively raise awareness of cybersecurity while exploring opportunities to expand deployment and utilization of transportation technologies?



TTSP Report Card, as of August 2023

Key	
	No role identified for NVTA
	Role identified for NVTA
	Some progress has been made
	Moderate progress has been made
	Substantial progress has been made
	Task has been completed

Strategy		NVTA Roles								
		Authority Roles			Shared Roles			Staff Roles		
Number	Name	Funding	Policy	Advocate	Champion	Facilitate	Stakeholder	Planning	Outreach/ Education	Observer
1	Reduce congestion and increase throughput									
2	Maximize access to jobs, employees and housing									
3	Maximize cybersecurity and privacy for members of the public									
4	Enhance operations of the multimodal transportation system through connectivity and automation									
5	Develop pricing mechanisms that manage travel demand and provide sustainable travel options									
6	Maximize the potential of physical and communication infrastructure to serve existing and emerging modes									
7	Enhance regional coordination and encourage interoperability in the transportation system									
8	Advance decarbonization of the transportation system									
9	Enhance mobility in the region through innovation and emerging technologies in transit									



Cyber Threats



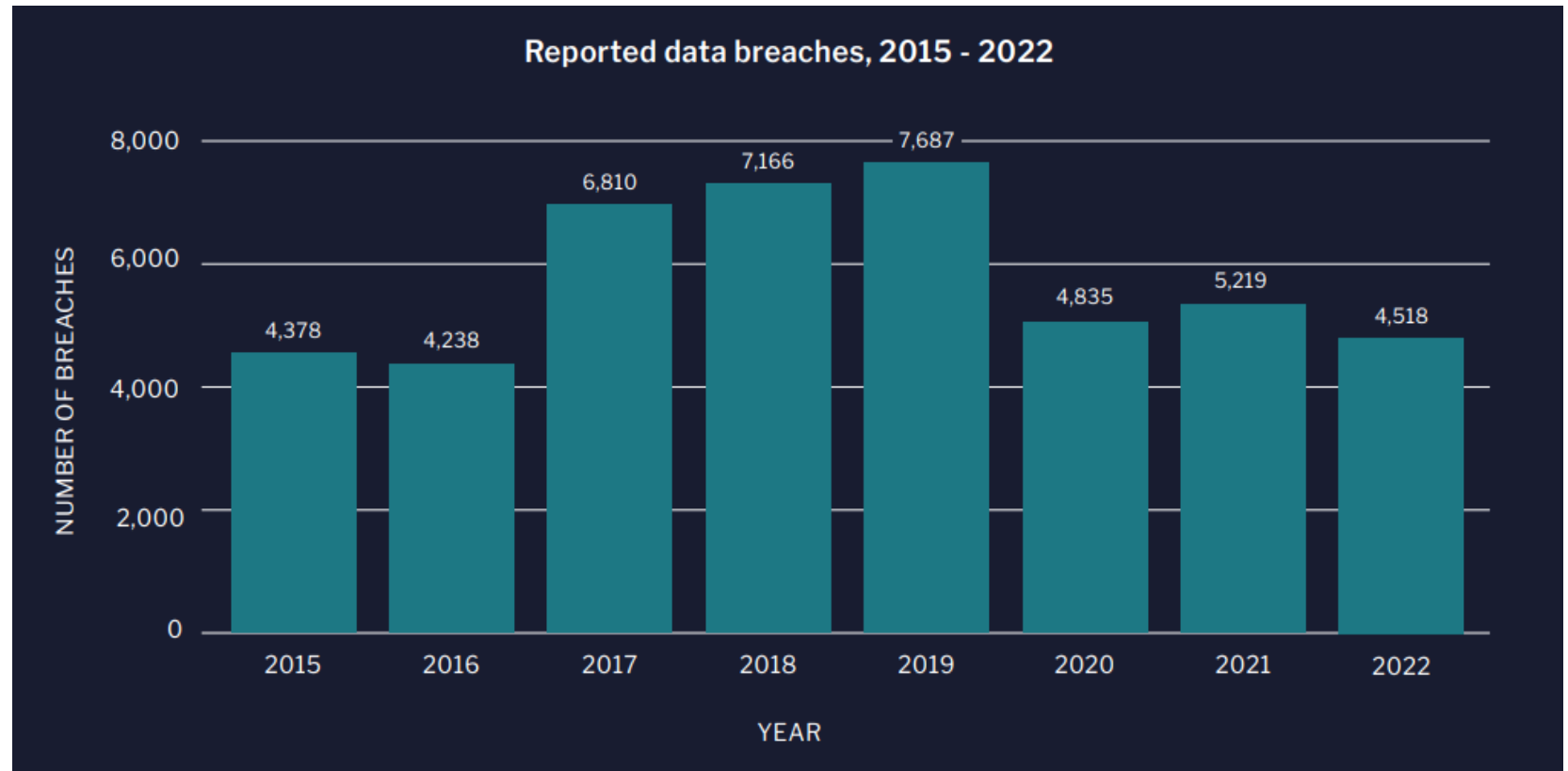
FBI CYBER

FBI Priorities

1. Counterterrorism
(International/Domestic)
2. Foreign Counterintelligence
- 3. Cyber Crime**
4. Public Corruption
5. Civil Rights
6. Transnational Criminal
Enterprise
7. White Collar Crime
8. Violent Crime

Cyber Actor's Goal

- The main goal of a cyber attack is to acquire information – names, passwords, financial records
- Information feeds the cyber criminal ecosystem

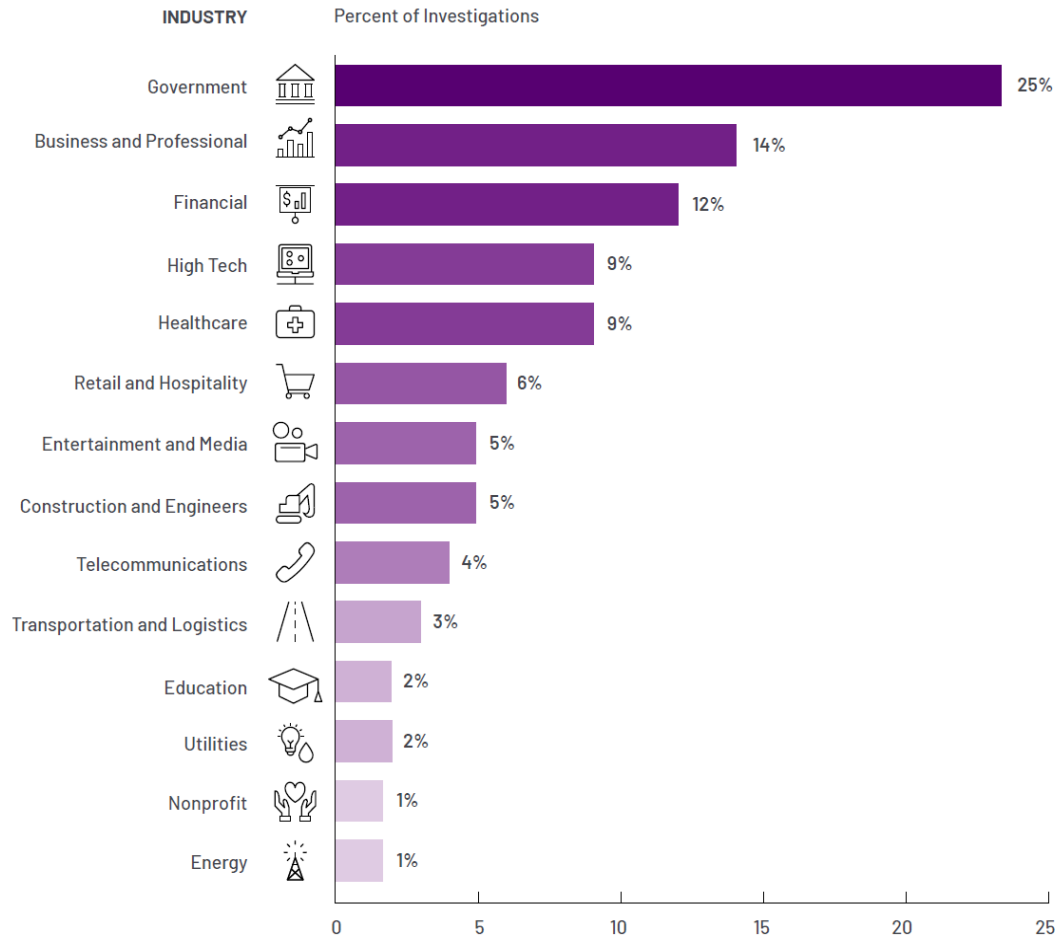


Source: "State of Cyber Threat Intelligence: 2023", Flashpoint



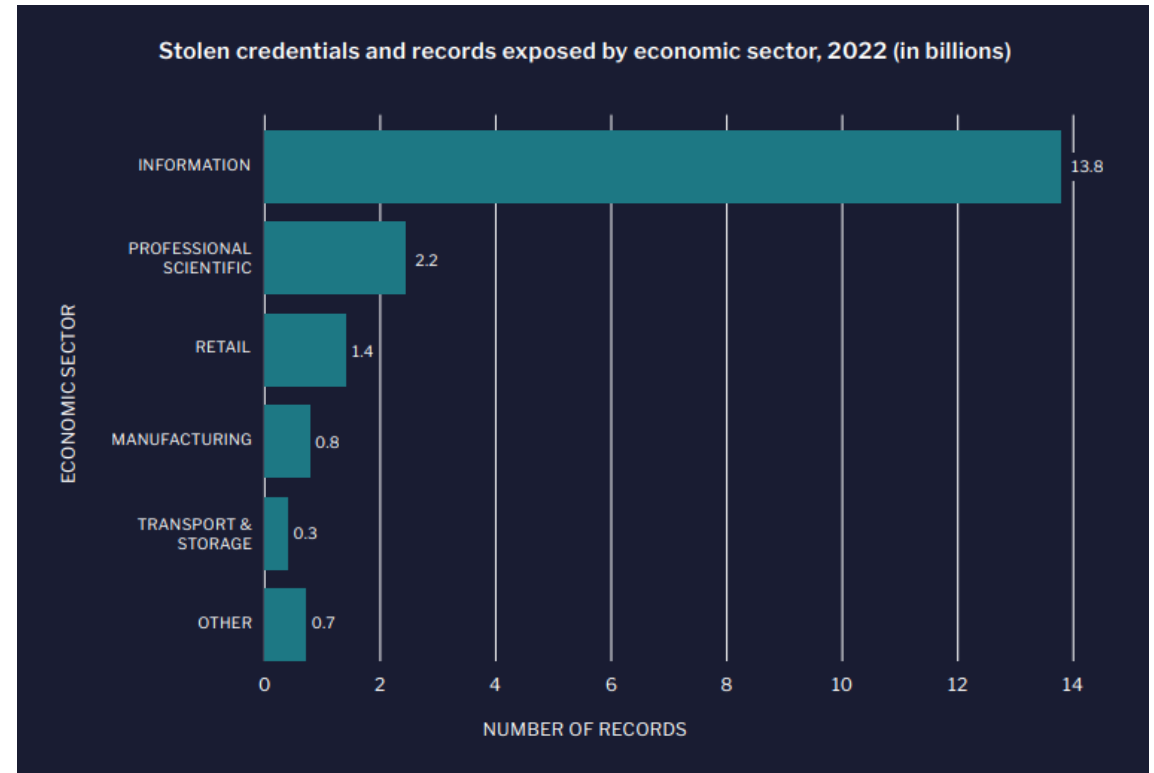
FBI CYBER

You Are the Targets?



Global Industries Targeted 2022







Source: Mandiant



Source: "State of Cyber Threat Intelligence: 2023", Flashpoint



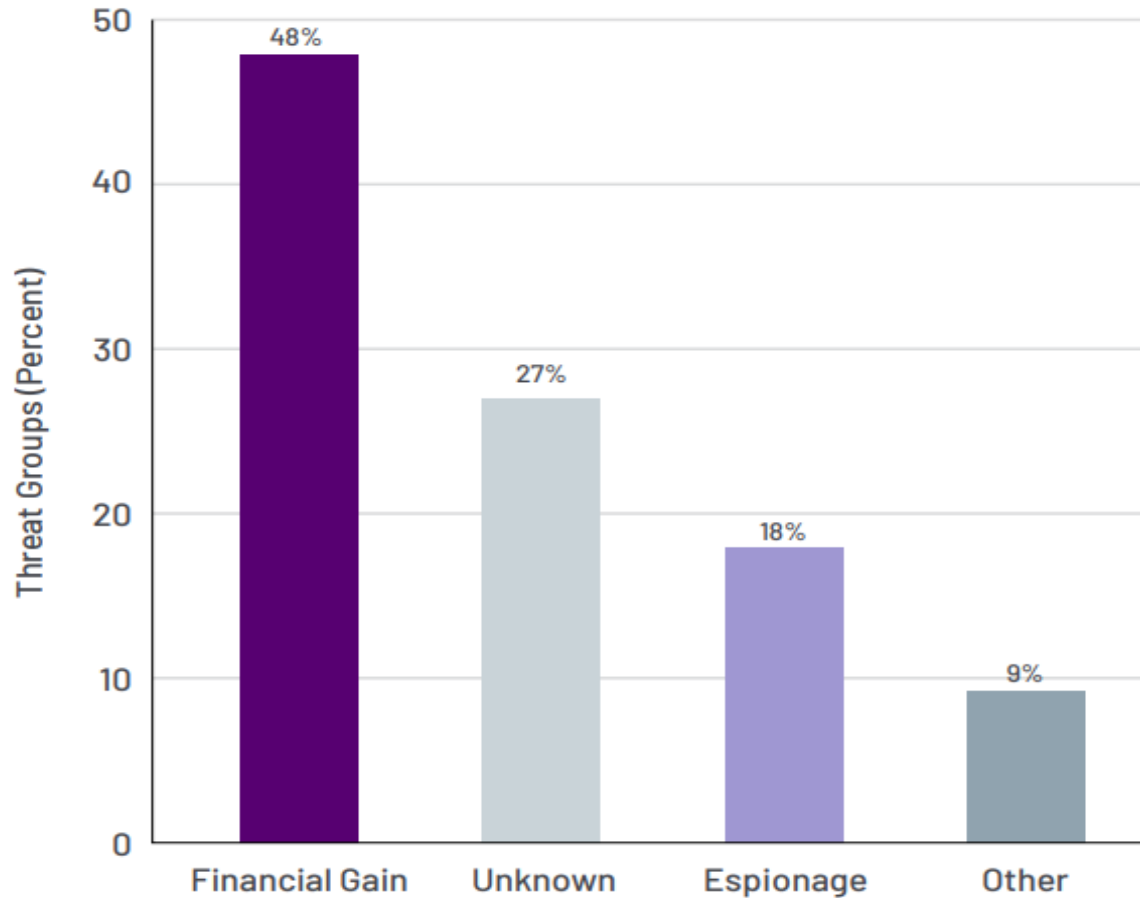
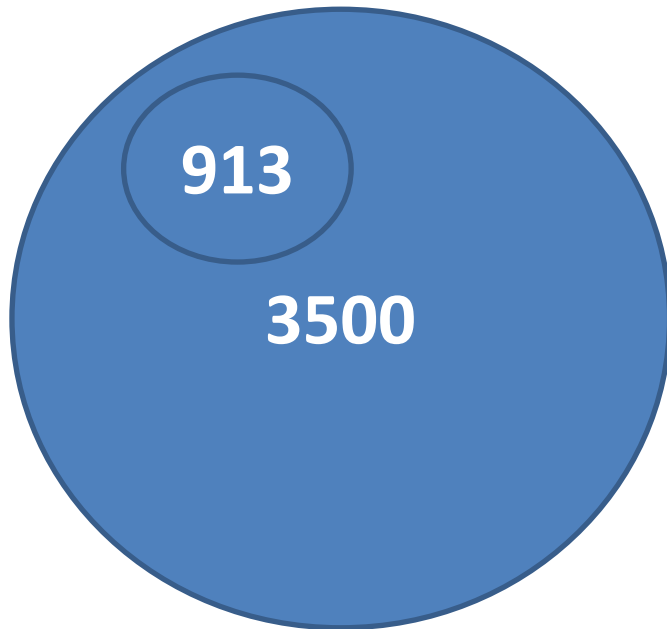
FBI CYBER

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Cyber Actor Threat Groups

Cyber Actor Threat Groups

Mandiant is tracking more than 3500 threat groups



"M-Trends 2023 Report" Mandiant

FBI CYBER

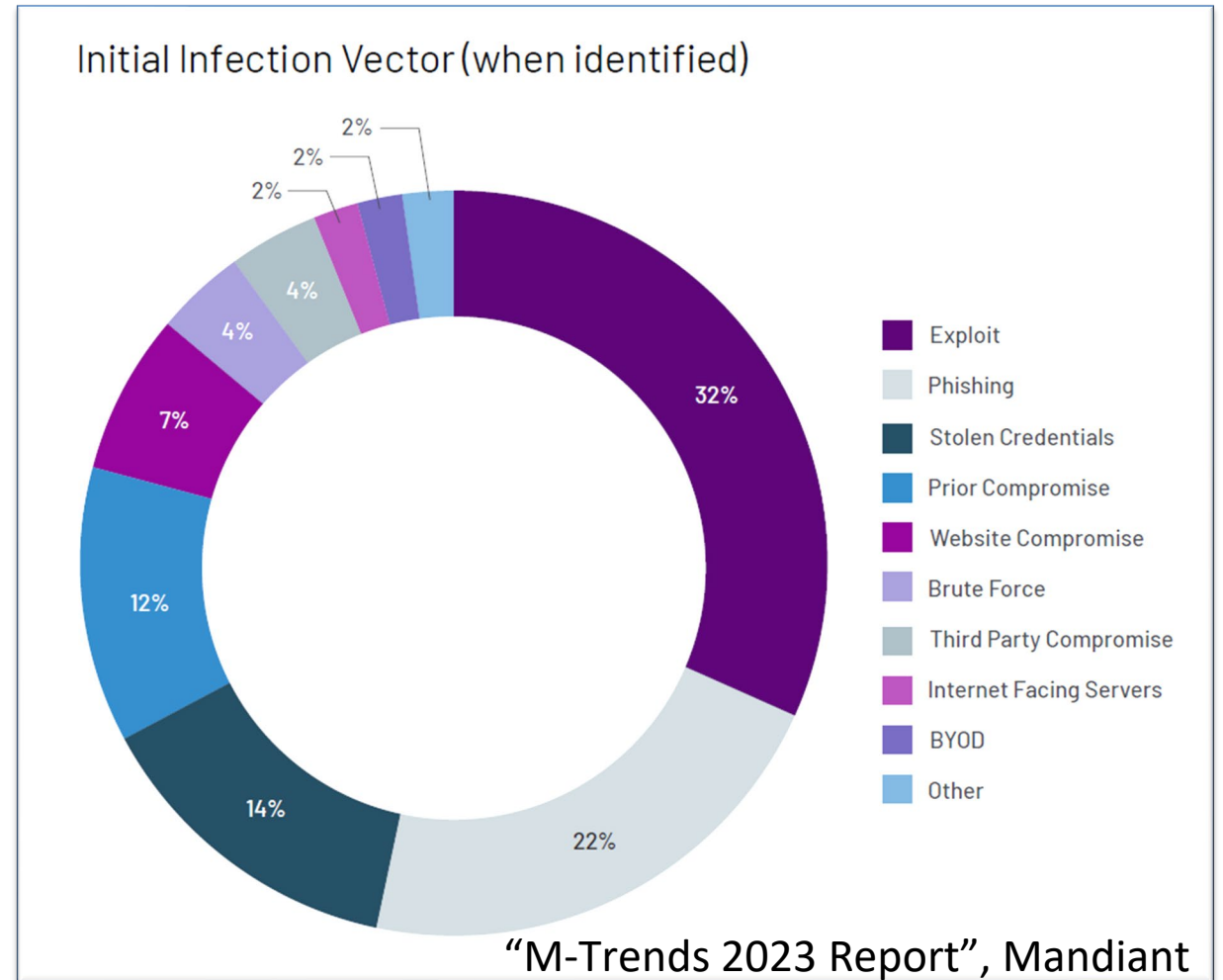


Initial Infection Vector

Top Vulnerabilities

Unpatched and
outdated systems

Lack of Education and
Training



FBI CYBER

Common Vulnerabilities and Exposures (CVE)

- Publicly disclosed security flaw
- Flashpoint collected 26,900 disclosed vulnerabilities this year — too many for one organization to patch in a timely manner
- Focus on CVEs being publicly discussed

According to Flashpoint's collections, there are over 306,000 known vulnerabilities—97,000 of which cannot be found in CVE and NVD.



F B I C Y B E R

Adversary Tactics

According to CrowdStrike, cyber actors continued to move beyond malware to gain initial access and persistence

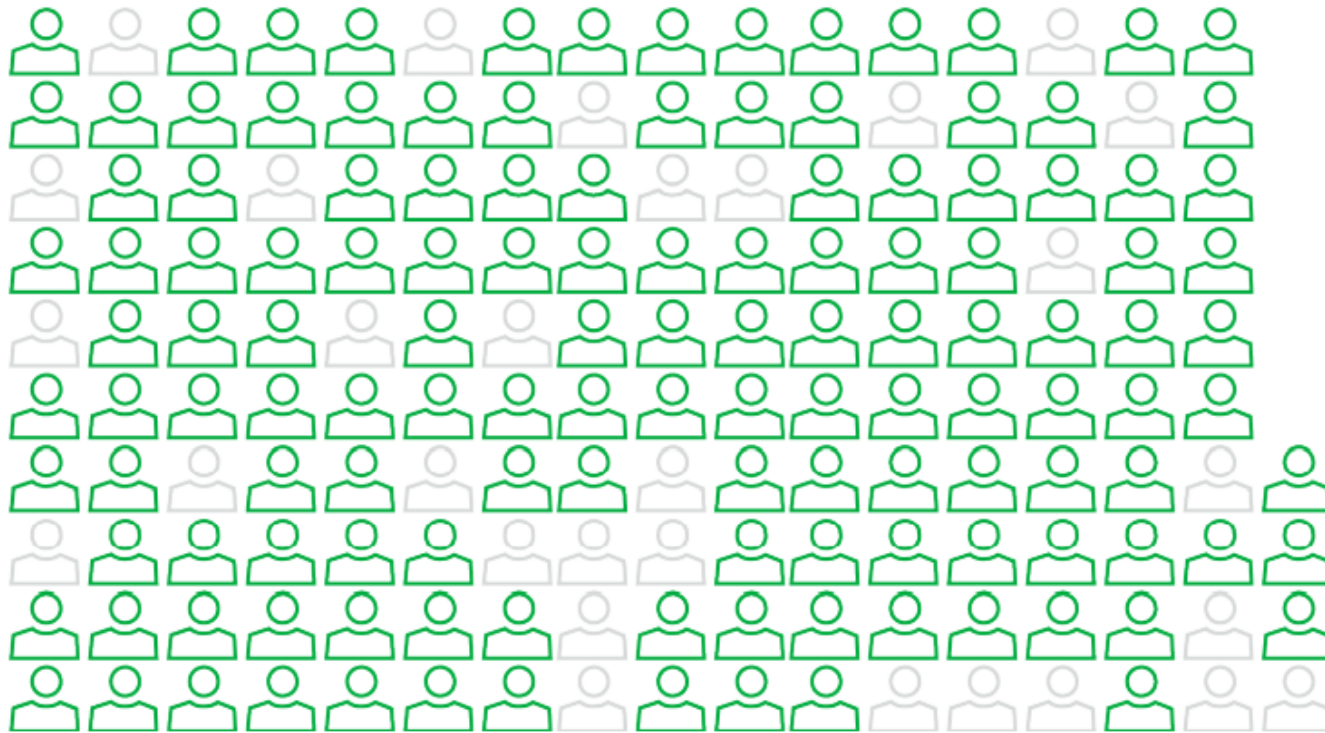
ADVERSARY TACTICS		■ Malware-Free
71%	2022	
62%	2021	
51%	2020	
40%	2019	
39%	2018	

Source: "2023 Global Threat Report", CrowdStrike



FBI CYBER

Users: The Biggest Vulnerability



The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

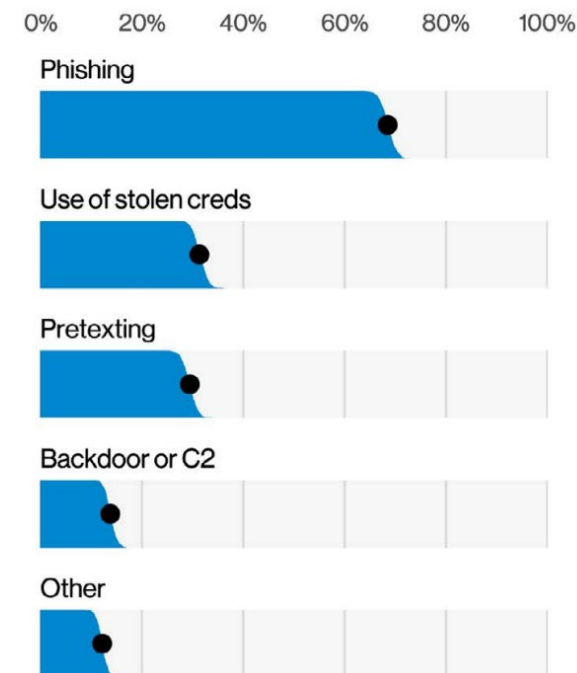


F B I C Y B E R

Source: “2022 Data Breach Investigations Report”, Verizon Corporation

Social Engineering

- The psychological manipulation of people into performing specified actions or divulging personal or confidential information



Source: “2022 Data Breach Investigations Report”,
Verizon Corporation



F B I C Y B E R

Phishing Effectiveness

- Campaign of just 10 emails yields greater than 90% success rate
- Average time from start of campaign to first compromise: 1 minute 22 seconds

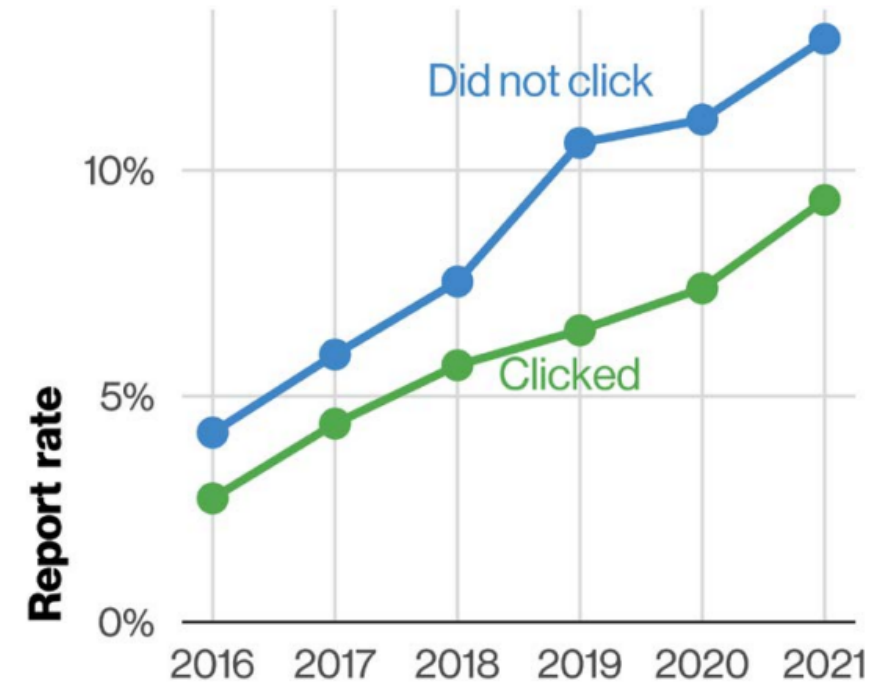


Figure 48. Phishing email report rate by click status (n=295,825,679)

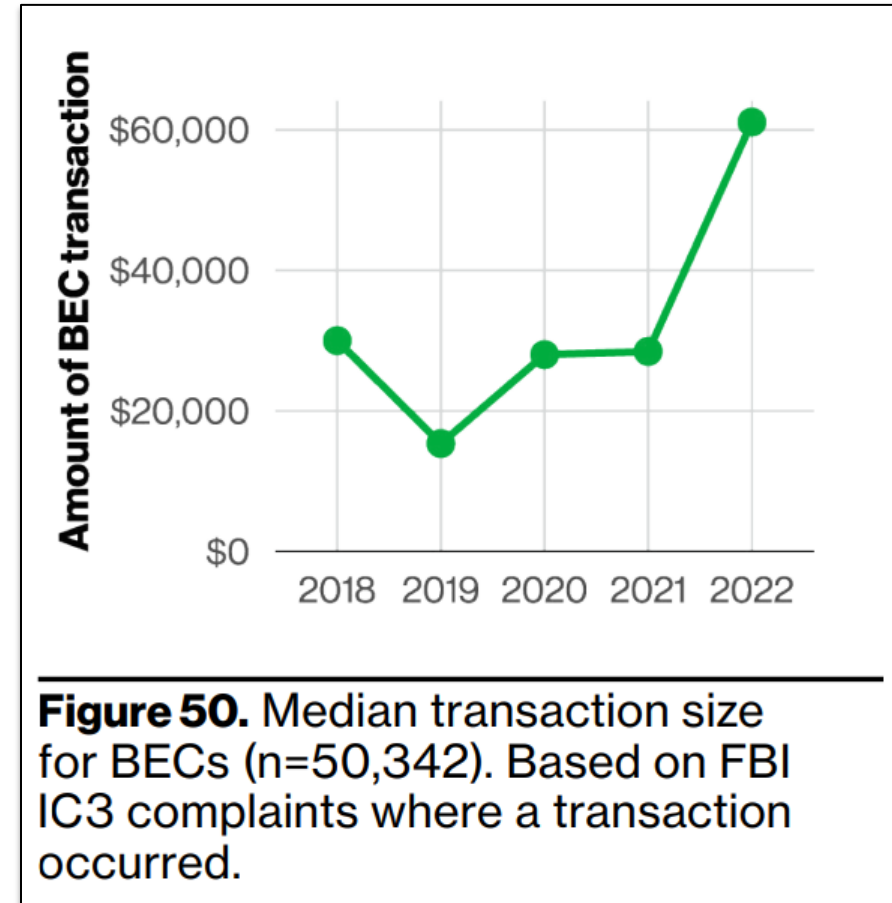


F B I C Y B E R

Source: “2022 Data Breach Investigations Report”, Verizon Corporation

Business Email Compromises

- Sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.
- Actors compromise or impersonate legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.



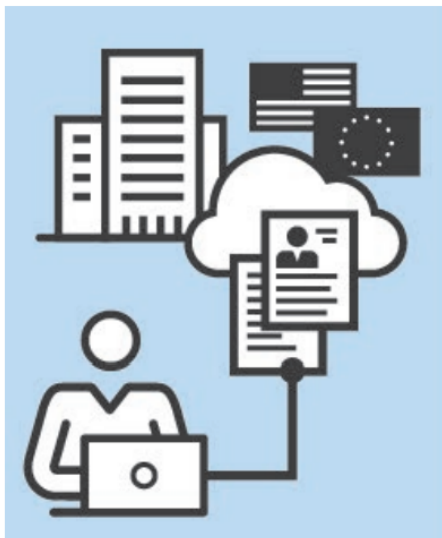
“2022 Data Breach Investigations Report” Verizon Corporation



F B I C Y B E R

Business Email Compromises

HOW IT OCCURS



Step 1

Identify Target

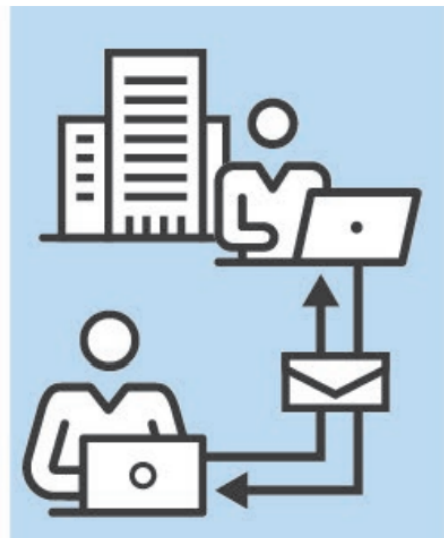
BEC actors target businesses and organizations, exploiting online information to develop a profile on the victim company and its executives.



Step 2

Grooming

Typically, someone in the finance department is targeted by spearphishing emails and/or phone calls. Criminal actors manipulate and exploit human nature through persuasion and pressure.



Step 3

Exchange of Information

With the victim convinced they are conducting a legitimate business transaction, they are provided with fraudulent wiring instructions.



Step 4

Wire Transfer

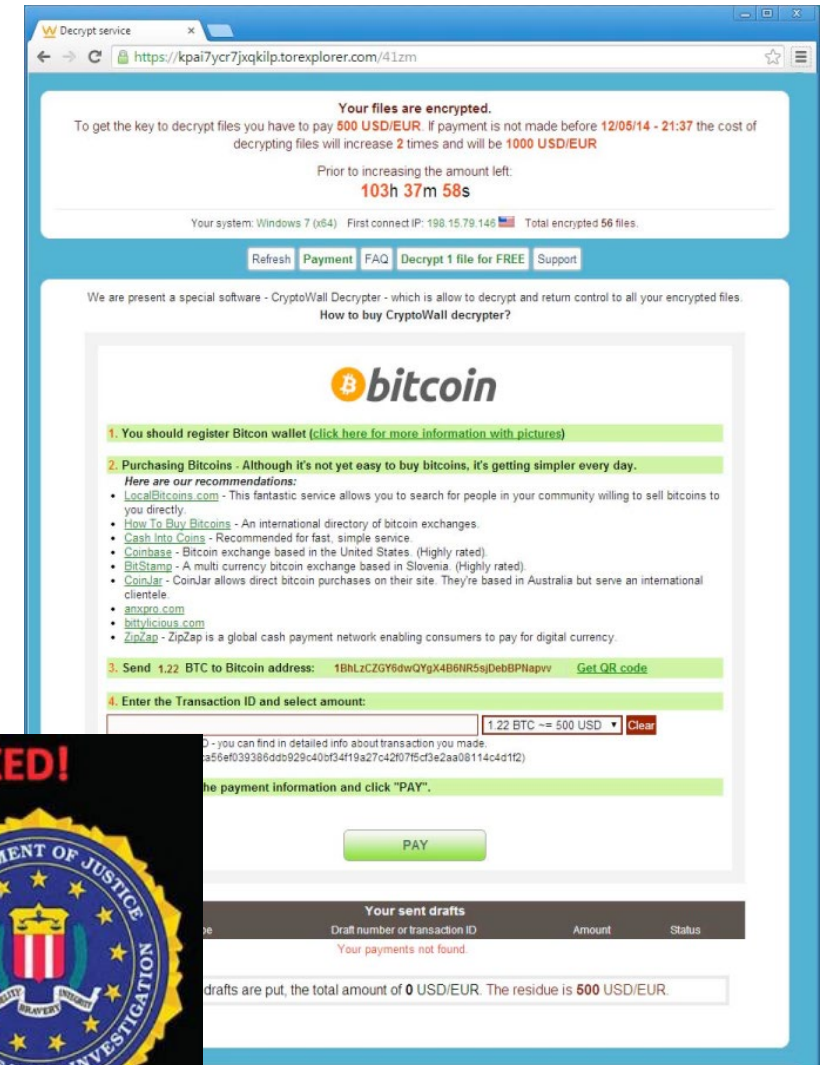
Upon transfer, the funds are steered to a bank account controlled by the BEC actors.



FBI CYBER

Ransomware

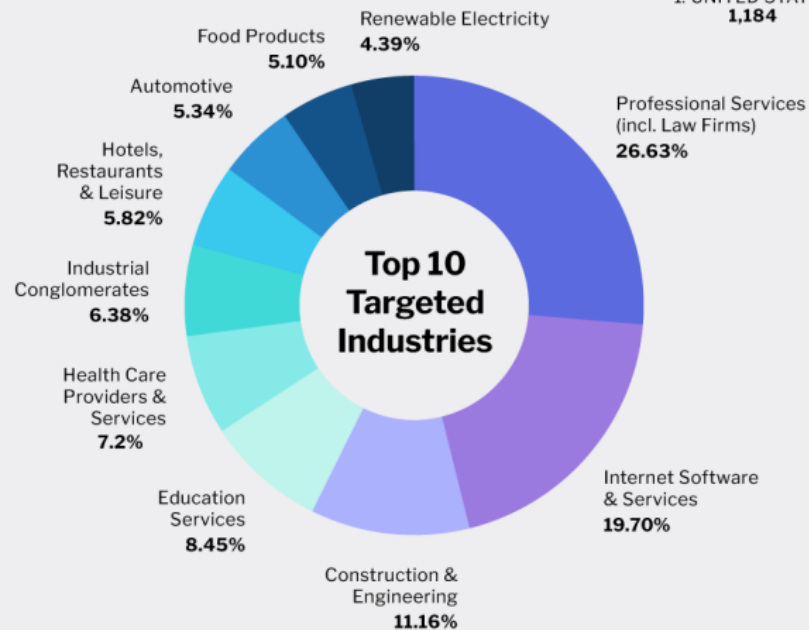
- Malware that encrypts data on a computer making it unusable.
- Actors hold data hostage until a ransom is paid.
- Actors apply additional pressure by threatening to delete or publicly release the victim's data.
- **The FBI does not encourage paying the ransom** because:
 - It encourages actors to attack again
 - It does not guarantee file recovery
 - Proceeds often fund illicit activities



F B I C Y B E R

Ransomware

State of Ransomware 2022



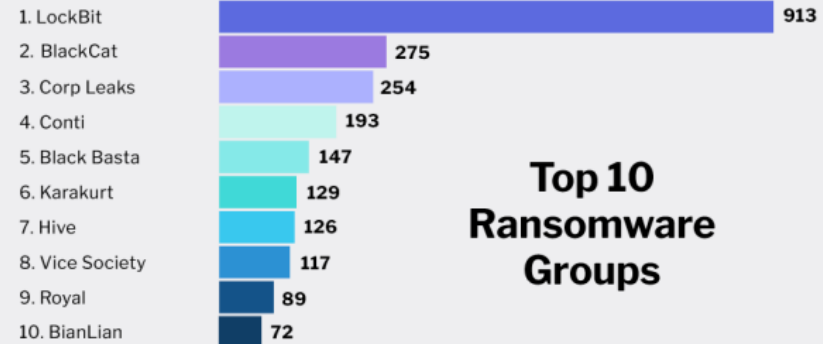
Top 12 Targeted Countries

LISTED IN ORDER WITH
NUMBER OF ATTACKS



RANSOMER NAME

VICTIM POSTS



Top 10 Ransomware Groups

© Copyright 2023 Flashpoint. Based on data from the Flashpoint Intelligence Platform | <https://flashpoint.io/platform/ransomware/>

FLASHPOINT



FBI CYBER

Minimizing Risks (Corporate)

- Anti-virus/malware/spyware, firewall
- Deploy patches quickly – 5 day window before exploited
- Use current software; minimum one generation behind (vendors stop distributing patches to older versions)
- User training
- Multi-factor authentication
- Encryption
- Know your assets



F B I C Y B E R

Minimizing Risks (Individual)

- Keep anti-virus/malware/spyware up to date
- Bank on a separate computer
- Use complex passwords
- Use caution on “open” networks
- Always review monthly statements carefully
- Check your credit reports annually
- Enable encryption on wireless routers
- Be suspicious of unsolicited e-mail with links
- Check web URLs and links very carefully



F B I C Y B E R

BEC: Minimizing Risk and Impact

- **Implement awareness and training programs:** All employees should go through regular training detailing the threat of BEC and how it is delivered, as well as best practices to prevent BEC by learning how to identify phishing emails and how to respond to suspected compromises.
- **Confirm payments via telephone prior to disbursing funds:** Require that the finance department contact vendors via the original phone numbers on file prior to transferring funds. Any phone numbers listed in a fund transfer request could be associated with the malicious actor.
- **Flag suspicious emails:** Create an email rule to flag email communications where the “reply” email address is different from the “from” email address shown.
- **Clearly distinguish between internal and external email senders:** Establish a warning notification that clearly distinguishes emails that originated from an external sender.



Ransomware: Minimizing Risk and Impact

- Backup your data, system images, and configurations
- Test your backups and keep them offline
- Utilize multifactor authentication
- Update and patch your systems
- Make sure your security solutions are fully up to date
- Review and exercise your incident response plan



F B I C Y B E R

When to Report?

- Electronic evidence dissipates over time, so **speed is essential** in a cyber intrusion investigation.
- Enlisting the FBI's help **as soon as an incident is discovered** enables quick investigative action and allows the preservation of evidence which increases the odds of a successful prosecution or other action to disrupt the perpetrators.
- **Develop a relationship with their local FBI field office prior to an incident.** Proactively building a relationship with the FBI provides companies with a dedicated FBI point-of-contact in the event of an incident and provides access to FBI cyber mitigation resources.



How Do I Report a Cyber Incident to the FBI?

FBI Field Offices

(local or international)
www.fbi.gov/contact-us

**FBI Internet Crime
Complaint Center (IC3)**
www.ic3.gov

Online Tips and Leads Form
tips.fbi.gov

FBI Tip Line

1-800-CALL-FBI
(1-800-225-5324)

CyWatch 24/7 Cyber Center
1-855-292-3937 or
cywatch@fbi.gov



FBI CYBER

What Should be Reported?

- Logs for the affected machines
- A timeline of events
- The identity of whoever reported the incident
- The identity of the victim of the incident
- The nature of the incident
- When the incident was initially detected
- How the incident was initially detected
- The actions that have already been taken
- Who has been notified of the incident



Why Should I Report?

In response to a reported cyber incident, the FBI may be able to:

- Identify and stop the activity. Potentially recover any transferred funds.
- Seize or disrupt the actor's technical infrastructure.
- Share valuable insights from other investigations that may help mitigate damage and prevent future incidents.
- Support your organization's data breach response.



F B I C Y B E R

How Will the FBI Protect Your Data and Interests?

- The FBI's efforts are directed towards the attacker and their actions on the system/network and not on the victim's defenses.
- The FBI works closely with the victim's legal counsel to address concerns.
- The FBI is mindful of the reputational harm that a cyber incident can cause.
- Often, the FBI requires only technical details to advance investigations not privileged communications or unrelated documents.
- FBI investigations are carefully coordinated with victim companies to minimize disruption to normal business operations.



F B I C Y B E R

Partnership is Critical

- Establish a relationship with your local FBI office prior to an incident
- Discuss your priorities and needs with the FBI
- Seek to understand the FBI's process



FBI CYBER



Questions?

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

**“DEFEND TODAY,
SECURE TOMORROW.”**



Ashley Jones

Cybersecurity State Advisor for the National Capital Region
Region III (MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

We lead the National effort
to understand, manage, and
reduce risk to our cyber and
physical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades

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



PARTNERSHIP
DEVELOPMENT



INFORMATION AND
DATA SHARING



CAPACITY BUILDING



INCIDENT
MANAGEMENT
& RESPONSE



RISK ASSESSMENT
AND ANALYSIS



NETWORK DEFENSE



EMERGENCY
COMMUNICATIONS

Critical Infrastructure Significance

- ✓ Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber
- ✓ So vital to the Nation, that their incapacitation or destruction would have a debilitating effect on:
 - National Security
 - The Economy
 - Public Health or Safety
 - Our Way of Life



KEY ACTIVITIES:



16 CRITICAL INFRASTRUCTURE SECTORS:



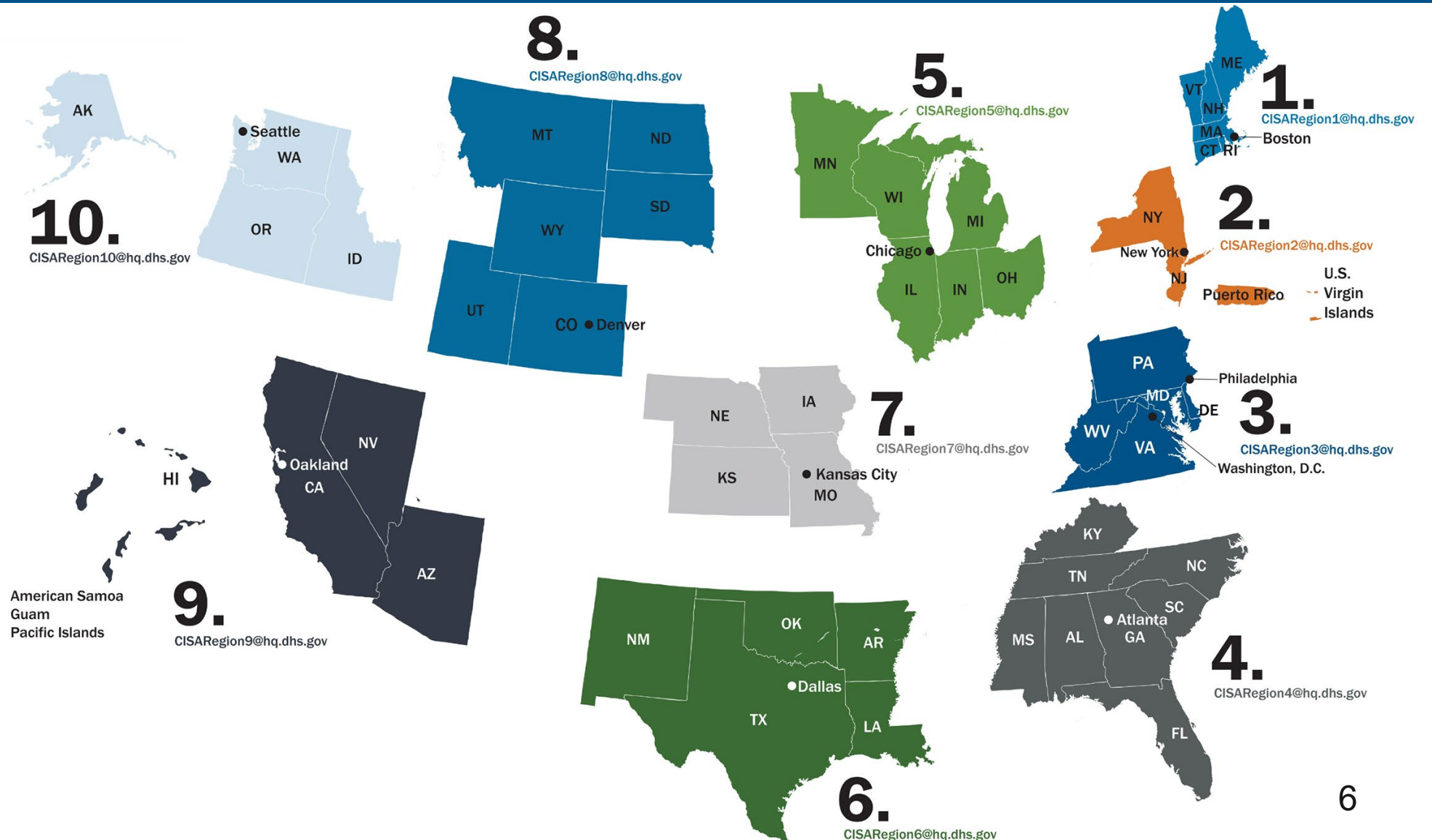
16 Critical Infrastructure Sectors & SRMAs

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA



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

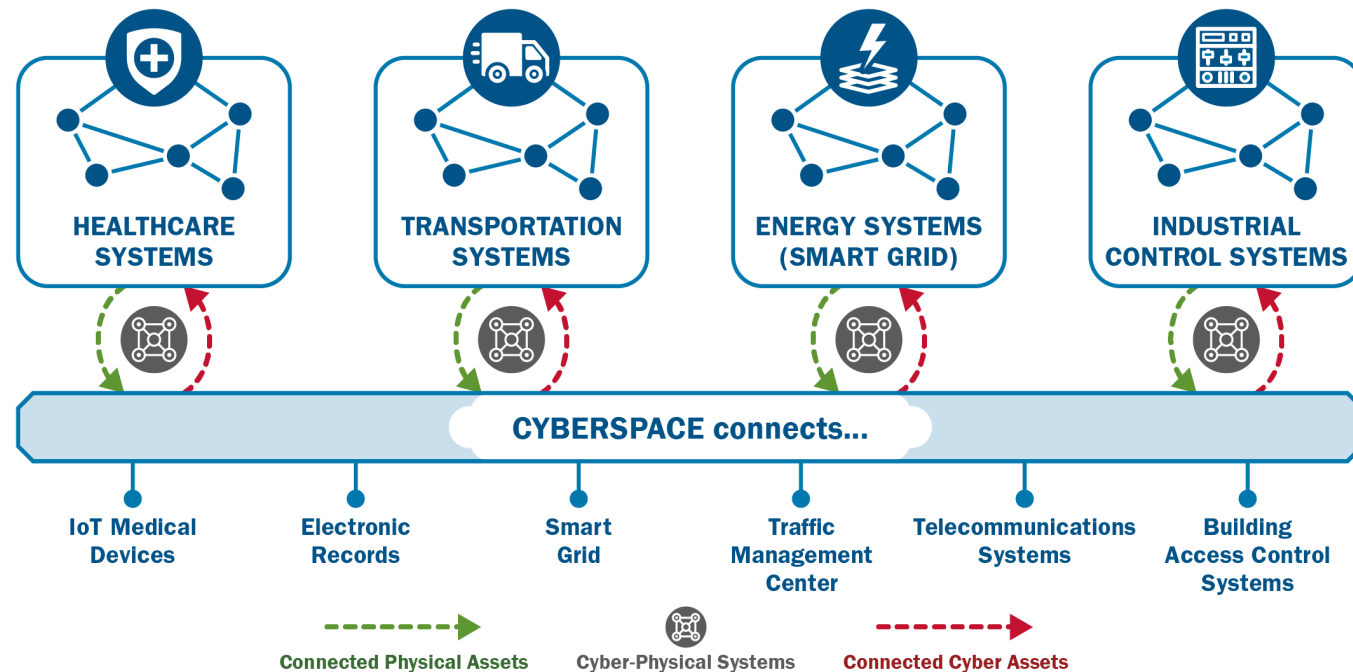
- Regional Director
- Deputy, Regional Director
- Chief, Protective Security Advisor
- **Protective Security Advisor (PSA)**
- Chief, Chemical Security Inspector
- **Chemical Security Inspector (CSI)**
- Senior Chemical Security Inspector
- Regional Operations Manager
- Critical Infrastructure Specialist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



Gray: Regional Office
Blue: Field Personnel

Cyber-Physical Convergence

Today's threats are targeting physical and cyber assets through sophisticated hybrid attacks with potentially devastating impacts to data, property and physical safety. CISA defines convergence as formal collaboration between previously disjointed security functions.



Protective Security Advisors

Five mission areas that directly support the protection of critical infrastructure

1. Plan, coordinate, and conduct security surveys and assessments (i.e., IST, SAFE)
2. Plan and conduct outreach activities
3. Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events
4. Respond to incidents
5. Coordinate and support improvised explosive device awareness and risk mitigation training



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
- 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



CISA Service Delivery Model

Regional Services

- Cyber Protective Visits -----
- Cyber Resilience Review -----
- External Dependencies Management Assessment -----
- Cyber Infrastructure Survey -----
- Workshops -----
 - Incident Management Workshop -----
 - Cyber Resilience Workshop -----
 - SLTT Cybersecurity Awareness Workshop -----
- Cyber Security Evaluations Tool (self-assessments) -----

STRATEGIC
(Management/C-Suite Level)



Enterprise Services

- Cyber Hygiene (Technical) -----
 - Vulnerability Scanning -----
 - Phishing Campaign Assessment -----
 - Web Application Scanning -----



National Services

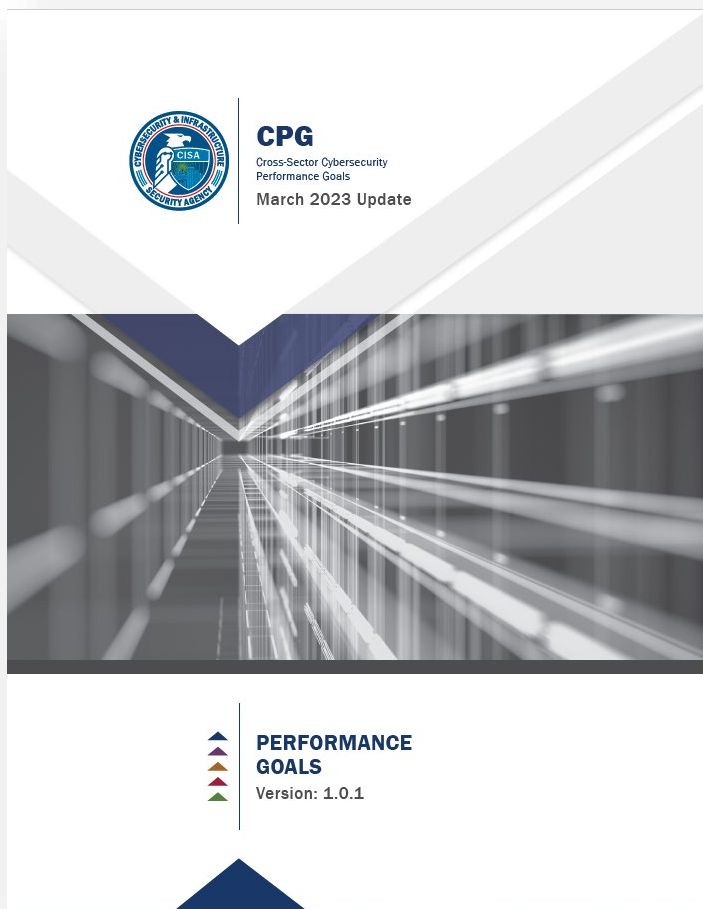
- Remote Penetration Test -----
- Risk and Vulnerability Assessment -----
- Validated Architecture Design Review -----
- Red Team Assessment -----



TECHNICAL
(Network-Administrator Level)



Cross-Sector Cybersecurity Performance Goals (CPG)

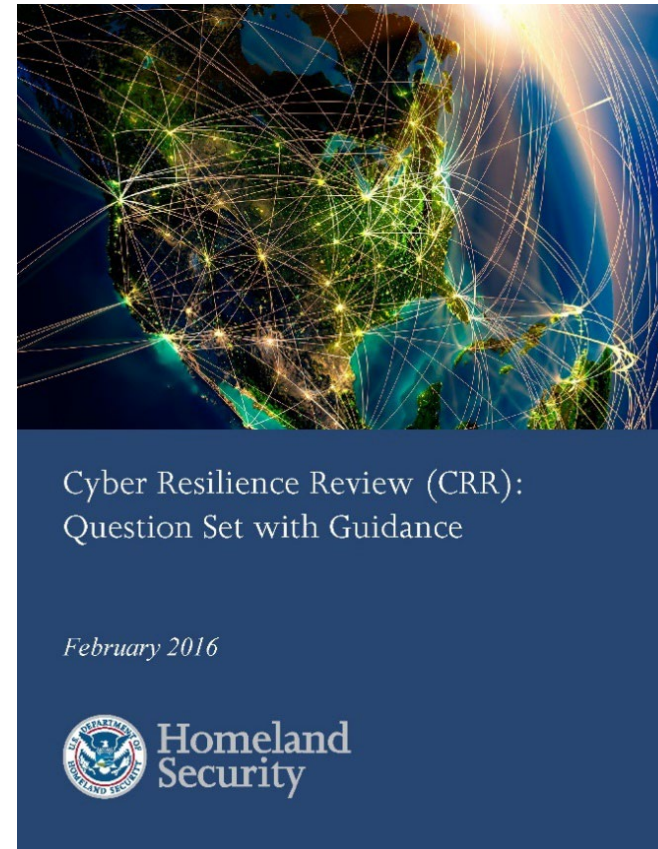


- Interview-based assessment of baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value:
 - Align to the NIST CSF functions of Identify, Protect, Detect, Respond, Recover (38 Questions)
 - A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
 - A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.
 - Available as: **CSA-facilitated**, or **self-assessment**
 - When facilitated, 2-person teams (*mastery level can conduct solo*)
 - **1-2** hours to complete and can be combined with a SAFE Assessment
 - CRR report

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services**.
- **Delivery:** Either CSA-facilitated, or self-administered
- **Benefits:** Report detailing an organizations capability and maturity in security management, and gaps against NIST CSF

*Voluntary assessment that is available at **no-cost** to requesting organizations*



CRR Question Set & Guidance

Cyber Resilience Review Domains

Asset Management

Know your assets being protected & their requirements, e.g., Confidentiality, Integrity, and Availability

Risk Management

Know and address your biggest risks that considers cost and your risk tolerances

Configuration and Change Management

Manage asset configurations and changes

Service Continuity Management

Ensure workable plans are in place to manage disruptions

Controls Management

Manage and monitor controls to ensure they are meeting your objectives

Situational Awareness

Discover and analyze information related to immediate operational stability and security

External Dependencies Management

Know your most important external entities and manage the risks posed to essential services

Training and Awareness

Ensure your people are trained on and aware of cybersecurity risks and practices

Incident Management

Be able to detect and respond to incidents

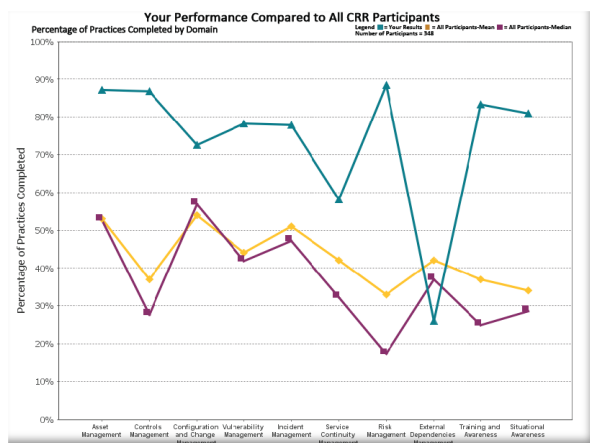
Vulnerability Management

Know your vulnerabilities and manage those that pose the most risk

For more information: <https://www.cisa.gov/cyber-resource-hub>



CRR Sample Report includes:



Comparison data with
other CRR participants
**facilitated only*



A summary “snapshot”
graphic, related to the **NIST
Cyber Security Framework**.

Domain performance of
existing cybersecurity
capability and options for
consideration for all responses

DOMAIN 1: ASSET MANAGEMENT									
MIL-1MIL-2MIL-3MIL-4MIL-5									
GE	GE	GE	GE	GE	GE	GE	GE	GE	GE
The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:									
<ul style="list-style-type: none">Goal 1 - Identify & prioritize critical servicesGoal 2 - Inventory assets, and establish the authority and responsibility for these assetsGoal 3 - Establish the relationship between assets and the services they supportGoal 4 - Manage the asset inventoryGoal 5 - Manage access to assetsGoal 6 - Prioritize & manage information assetsGoal 7 - Prioritize & manage facility assets									
The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.									
Goal 1 - Identify & prioritize critical services									
1. Are critical services identified? [SC.SG2.SP1]									
								Yes	
2. Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC.SG2.SP1]									
								Incomplete	
Goal 2 - Inventory assets, and establish the authority and responsibility for these assets									
1. Are the assets that directly support the critical service inventoried? [ADM.SG1.SP1]									
								People	Incomplete
								Information	Incomplete
								Technology	Incomplete
								Facilities	Yes
Goal 3 - Establish the relationship between assets and the services they support									
Q1 CERT-RMM Reference: [ADM.SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support.									
Additional Reference: NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)									



Protected Critical Infrastructure Information

- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes.
- PCII protects from release through:
 - ✓ Freedom of Information Act disclosure requests
 - ✓ State, local, tribal, territorial disclosure laws
 - ✓ Use in civil litigation
 - ✓ Use for regulatory purposes



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION Requirements for Use	
Nondisclosure	
<p>This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.</p> <p>By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.</p> <p>If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.</p>	
Access	<p>Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:</p> <ul style="list-style-type: none">• Assigned to homeland security duties related to this critical infrastructure; and• Demonstrate a valid need-to-know. <p>The recipient must comply with the requirements stated in the CII Act and the Regulation.</p>
Handling	<p>Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. Do not leave this document unattended.</p> <p>Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.</p> <p>Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.</p> <p>Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. Do not send PCII to personal, non-employment related email accounts. Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.</p> <p>Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "POSTMASTER: DO NOT FORWARD. RETURN TO SENDER." Adhere to the aforementioned requirements for interoffice mail.</p> <p>Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.</p> <p>Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.</p> <p>Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.</p> <p>Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.</p>
Sanitized Products	<p>You may use PCII to create a work product. The product must not reveal any information that:</p> <ul style="list-style-type: none">• Is proprietary, business sensitive, or trade secret;• Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and• Is otherwise not appropriately in the public domain.
Derivative Products	<p>Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.</p> <p>For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.</p>
Submission Identification Number: <input type="text"/>	
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION	

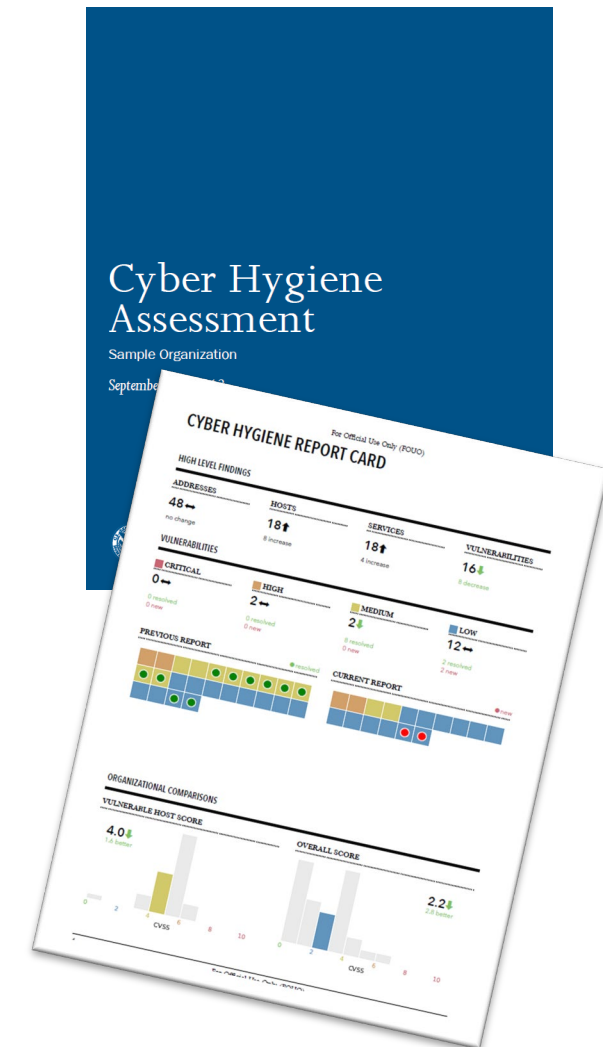
CyHy - Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

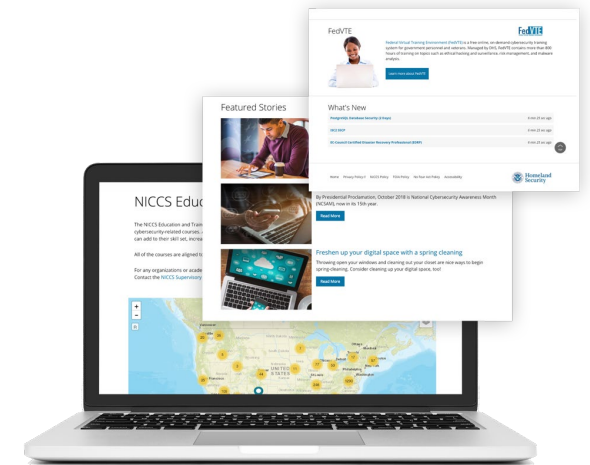
- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness
- Email us at vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.



Cybersecurity Training Resources

CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

- **The NICCS website:** Searchable Training Catalog with over 6,000 cyber-related courses offered by nationwide cybersecurity educators
 - Interactive National Cybersecurity Workforce Framework
 - **FedVTE**
 - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
 - Tools and resources for cyber managers
- Incident Response Training through IMR Series
- Industrial Control Systems (ICS) Training



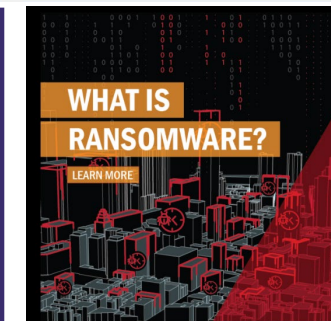
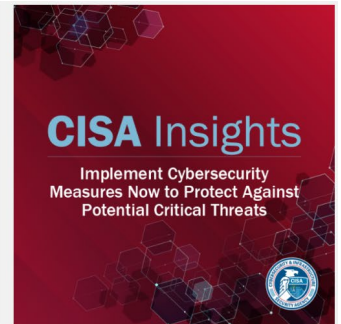
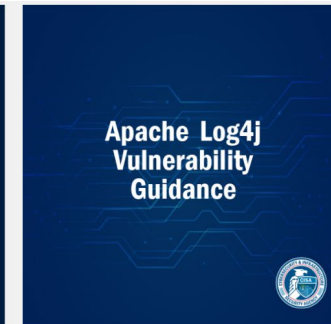
IDENTIFY				MITIGATE				RECOVER			
Awareness Webinars: Guidance for organizational readiness and best practices				Cyber Range Training: Skill development through step-action labs				Cyber Range Challenges: Live incident response scenarios for experienced practitioners			
Open to ALL levels				Open to ALL levels				Intermediate to Advanced			
no cap				cap ~35				cap ~50			
1hr event				4hr event				8hr event			



For more information, visit
<https://www.cisa.gov/cybersecurity-training-exercises>

Recent CISA Resources:

- Incident and Vulnerability Response Playbooks:
https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- Known Exploited Vulnerabilities Catalog:
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Cyber Incident Resource Guide for Governors:
https://www.cisa.gov/gov_cyberguide
- Stop Ransomware:
<https://www.cisa.gov/stopransomware>
- Cyber Training, Exercises, Tabletops:
<https://www.cisa.gov/cybersecurity-training-exercises>
- Free Cyber Tools and Services:
<https://www.cisa.gov/free-cybersecurity-services-and-tools>



Additional CISA Resources:

- **CSET Tool Download:** <https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr>
- **Cyber Hygiene Services:** email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.
- **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-packages>
- **Known Exploited Vulnerabilities (KEV) Catalog:** <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- **Cyber Incident Response :** <https://us-cert.cisa.gov/forms/report> and/or **Filing a Complaint with IC3:** <https://www.ic3.gov/>



Additional Information Sharing Opportunities

- **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



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



- **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.



ONG-ISAC



National Defense ISAC



RETAIL & HOSPITALITY
ISAC



Real Estate
ISAC
Information Sharing
and Analysis Center
Serving the Commercial Facilities Sector





Ashley Jones

Cybersecurity Advisor, Region 3

National Capitol Region

Ashley.Jones@cisa.dhs.gov

Regional Support:

CISARegion3@hq.dhs.gov

To Report an Incident:

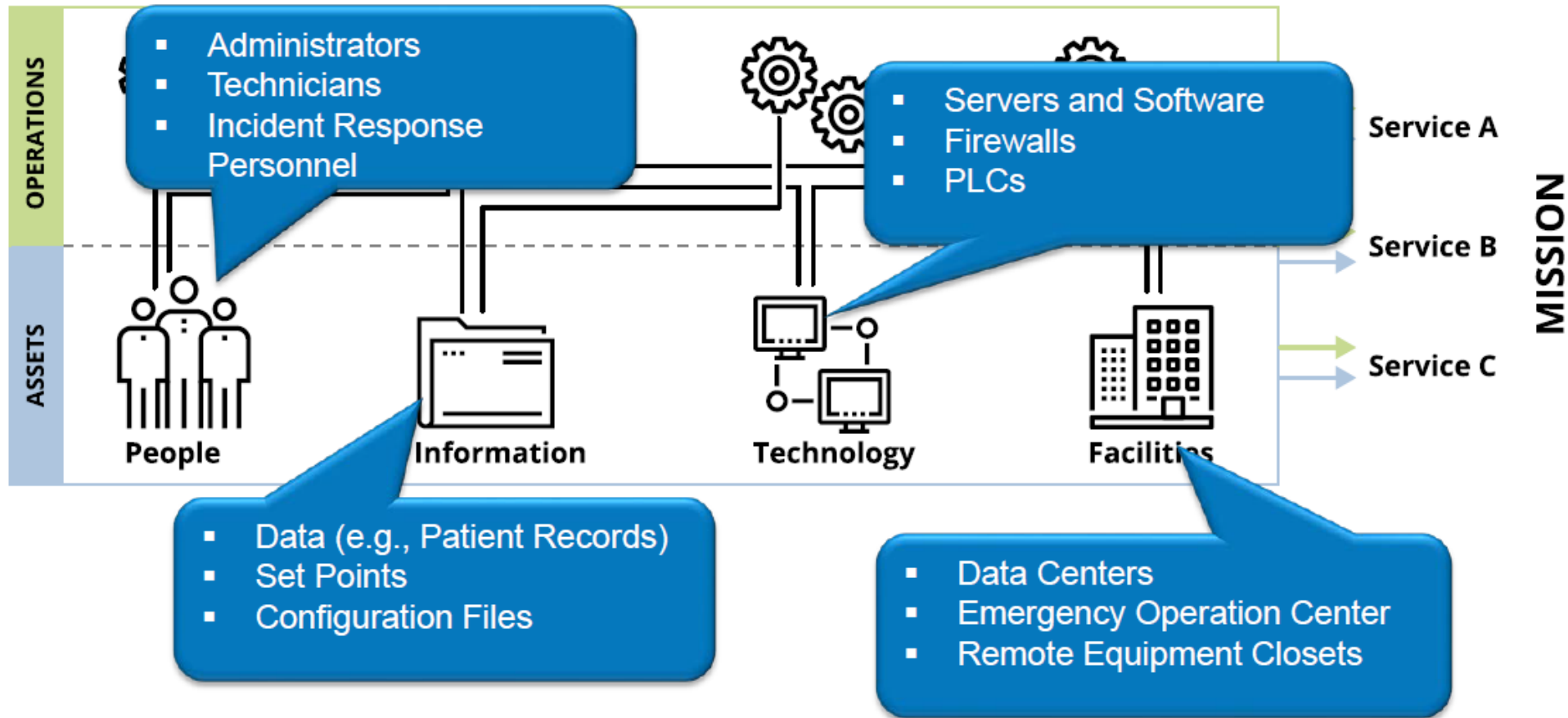
<https://us-cert.cisa.gov/report>

Media Inquiries:

CISAMedia@cisa.dhs.gov



Critical Service Assets and Examples





Item IV: NVTA's InNoVations Initiatives Poster



Northern Virginia Transportation Authority's InNoVation Initiatives

The Northern Virginia Transportation Authority (NVTA) is committed to taking a proactive approach to technology to build momentum for the innovative transportation system of tomorrow.

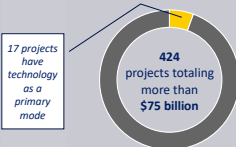


BUILDING MOMENTUM

NVTA's TransAction

The Northern Virginia Transportation Authority (NVTA) develops Northern Virginia's long-range transportation plan, called TransAction. TransAction addresses regional transportation needs by identifying transportation projects that reduce congestion, enhance mobility, increase accessibility, and improve resiliency. The findings in TransAction are used to inform the NVTA's Six Year Program for Regional Revenue funding.

TransAction includes:

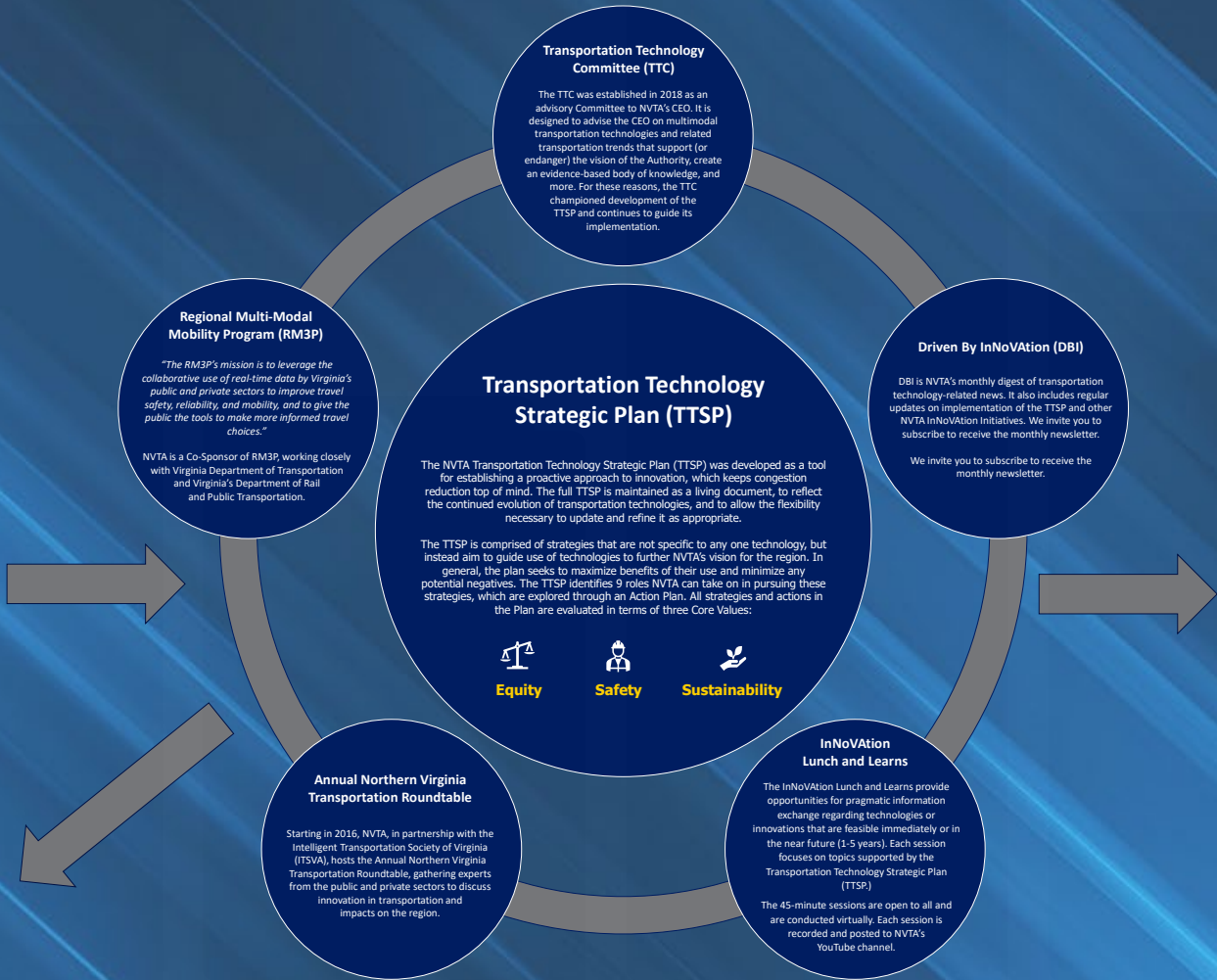


TransAction Vision Statement:

"Northern Virginia will plan for, and invest in, an Equitable, Safe, Sustainable, and integrated multimodal transportation system that enhances quality of life, strengthens the economy, and builds resilience."

NVTA's Legislative Priorities

A legislative priority to "Support use of effective transportation technology" was introduced into NVTA's State and Federal Legislative Program in 2022. The position has since been updated and continued.



NVTA's Six Year Program

NVTA allocates Regional Revenues to transportation projects across Northern Virginia during its Six Year Program (SYP) update that occurs every two years. The process begins with a Call for Regional Transportation Projects which allows eligible entities to apply for funding to advance projects from TransAction that align with regional transportation priorities.

NVTA has funded technology-related project(s) in each of its funding programs:



Scan this QR Code to learn more about NVTA's InNoVation Initiatives!



Item V: TTSP Recap



What is the Transportation Technology Strategic Plan (TTSP)?

- Tool that informs a proactive approach to adoption of transportation technology;
- TTSP considers how transportation technologies support the region's vision, i.e., needs-driven NOT technology-driven;
- Includes nine strategies, and up to nine NVTA roles for each strategy;
- TTSP is a living document that will be updated as transportation technologies evolve;
- TTSP Action Plan enables NVTA to think big, start small, and build momentum with respect to adoption of transportation technologies in the region.



History of the Transportation Technology Strategic Plan (TTSP)

The TTSP describes **strategies** for advancing the beneficial use of technology in transportation, in **alignment with NVTa Core Values**, and identified **roles the NVTa can take** in pursuit of them.

It also recognizes that the objectives of the TTSP cannot be achieved by NVTa alone and relies on the **strong coordination and partnerships** that are foundational to NVTa's work in the region.

Year	Month	Milestone
2017	October	An update to TransAction was adopted, which contained the genesis of the Transportation Technology Committee (TTC).
2018	October	TTC established by the NVTa CEO.
2019	January	Meeting: First meeting of the NVTa Transportation Technology Committee.
2020	December	Draft TTSP "core content" (8 strategies, 9 NVTa roles and 3 core values) shared with the TTC. The Authority unanimously voted to approve a revised vision statement for TransAction.
2021	January	Meeting: Draft structure for the TTSP (minus Action Plan) proposed to the TTC.
	February/ March	Meeting: First full draft of the TTSP and draft structure for the Action Plan presented to the TTC. Meeting: Draft structure for the TTSP shared with TAC, PCAC and PPC. TTSP mini-session at the 6 th annual NoVA Transportation Roundtable.
	April	Meeting: TTC, PCAC and PPC all recommend the Authority adopt the 8 strategies and Action Plans of the TTSP.
	May	The Authority adopted the inaugural NVTa Transportation Technology Strategic Plan's Action Plan and 8 Strategies within.
	Summer	TTSP-related topics included in TransAction outreach and survey.
	October	NVTa's Transportation Technology webpage is launched.
	December	The Authority unanimously adopted the 2022 State and Federal Legislative Program and Legislative Priorities, which included a new position to "Support use of effective transportation technology".
2022	February	The format of NVTa's Driven By InNoVation was updated and to include monthly features of TTSP-related content.
	April	Update: A Technology Timeline was introduced into the TTSP. Other small updates were also made.
	July	Meeting: The TTC unanimously voted to endorse expansion of the scope of strategies 4 and 8, and to add a 9 th strategy. Trial run of a series of InNoVation Lunch and Learn begins. There were three sessions, held in October, November and December. These were not recorded.
		Update: The TTSP was updated to reflect adoption of the updated TransAction goals.
	November	Update (substantive): The Authority unanimously approved expansion of the scope of strategies 4 and 8, and addition of a 9th strategy.
	December	The Authority unanimously adopted the 2023 State and Federal Legislative Program and Legislative Priorities, which continued the position to "Support use of effective transportation technology".
2023	April	First season of InNoVation Lunch and Learns begin. There were three sessions, held in May, June and July. These sessions were promoted publicly, recorded and posted on NVTa's YouTube page.
	September	Update (substantive, continued): Content to support the expansion of strategies 4 and 8, and addition of strategy 9 was completed.



TTSP Report Card, as of August 2023

Key	
	No role identified for NVTA
	Role identified for NVTA
	Some progress has been made
	Moderate progress has been made
	Substantial progress has been made
	Task has been completed

Strategy		NVTA Roles								
		Authority Roles			Shared Roles			Staff Roles		
Number	Name	Funding	Policy	Advocate	Champion	Facilitate	Stakeholder	Planning	Outreach/ Education	Observer
1	Reduce congestion and increase throughput									
2	Maximize access to jobs, employees and housing									
3	Maximize cybersecurity and privacy for members of the public									
4	Enhance operations of the multimodal transportation system through connectivity and automation									
5	Develop pricing mechanisms that manage travel demand and provide sustainable travel options									
6	Maximize the potential of physical and communication infrastructure to serve existing and emerging modes									
7	Enhance regional coordination and encourage interoperability in the transportation system									
8	Advance decarbonization of the transportation system									
9	Enhance mobility in the region through innovation and emerging technologies in transit									



Item VI: Artificial Intelligence in Transportation



What is Artificial Intelligence (AI)?

"Artificial intelligence is the capability of a computer system to mimic human cognitive functions such as learning and problem-solving. Through AI, a computer system uses math and logic to simulate the reasoning that people use to learn from new information and make decisions." – Microsoft

Discussion of Artificial Intelligence

- Possible near-term applications that support NVTA's vision
 - NVTA is a Co-sponsor of RM3P (Regional Multi-Modal Mobility Program), which includes an AI-Based Decision Support System. This could enhance the multimodal transportation system through connectivity and automation (TTSP strategy #4) and contribute to regional coordination and interoperability (TTSP strategy #7.)
 - AI can be used to optimize traffic management through signal timing and help reduce congestion and advance NVTA's Core Values of Safety and Sustainability.
- What keeps us up at night
 - AI that has been trained on/is referencing datasets that are not representative of the population or otherwise contain biased information, being used in critical decision-making processes.
 - The benefits of AI in transportation being concentrated in geographic areas and/or with demographic groups.



Discussion of Artificial Intelligence

Suggestion for NVTA’s role:

- Continue to monitor developments around AI and create educational opportunities.
- Consider incorporating AI into the TTSP, either as a technology or a new strategy.
- Evaluate if any other action is appropriate under the current TTSP, including updates to NVTA’s technology-related legislative priorities.

Technology	TTSP Strategies								
	1	2	3	4	5	6	7	8	9
	Reduce congestion and increase throughput	Maximize access to jobs, employees and housing	Maximize cybersecurity and privacy for members of the public	Enhance operations of the multimodal transportation system through connectivity and automation	Develop pricing mechanisms that manage travel demand and provide sustainable travel options	Maximize the potential of physical and communication infrastructure to serve existing and emerging modes	Enhance regional coordination and encourage interoperability in the transportation system	Advance decarbonization of the transportation system	Enhance mobility in the region through innovation and emerging technologies in transit
Artificial Intelligence	●		○	●	○		○		

Key					
Will definitely be helpful	Potential to be helpful	Equal potential to be helpful or detrimental	Potential to be detrimental	Likely to be detrimental	Not applicable or Insufficient Information
●	○	○	○	○	



Thank you!