Measuring our Agency's Cybersecurity Program

May 2023

Topics

- What is cybersecurity?
- What we have done so far?
- What's next?

INTERcity TRANSIT

What is cybersecurity?

Definition from CISA (US Department of Homeland Security – Cybersecurity & Infrastructure Security Agency)

- The art of protecting networks, devices, and data from unauthorized access or criminal use
- The practice of ensuring confidentiality, integrity, and availability of information

INTERcity TRANSIT

What is an effective cybersecurity program?

1. Senior Management provides clear direction on how to address cybersecurity.
2. All departments identify their valuable information assets and the technology used to handle it.
3. Cybersecurity staff assesses the risk of each information asset and develops policies to encourage secure use.
4. IS staff implement reasonable controls to automate security.

INTERcity TRANSIT

What we have done so far?

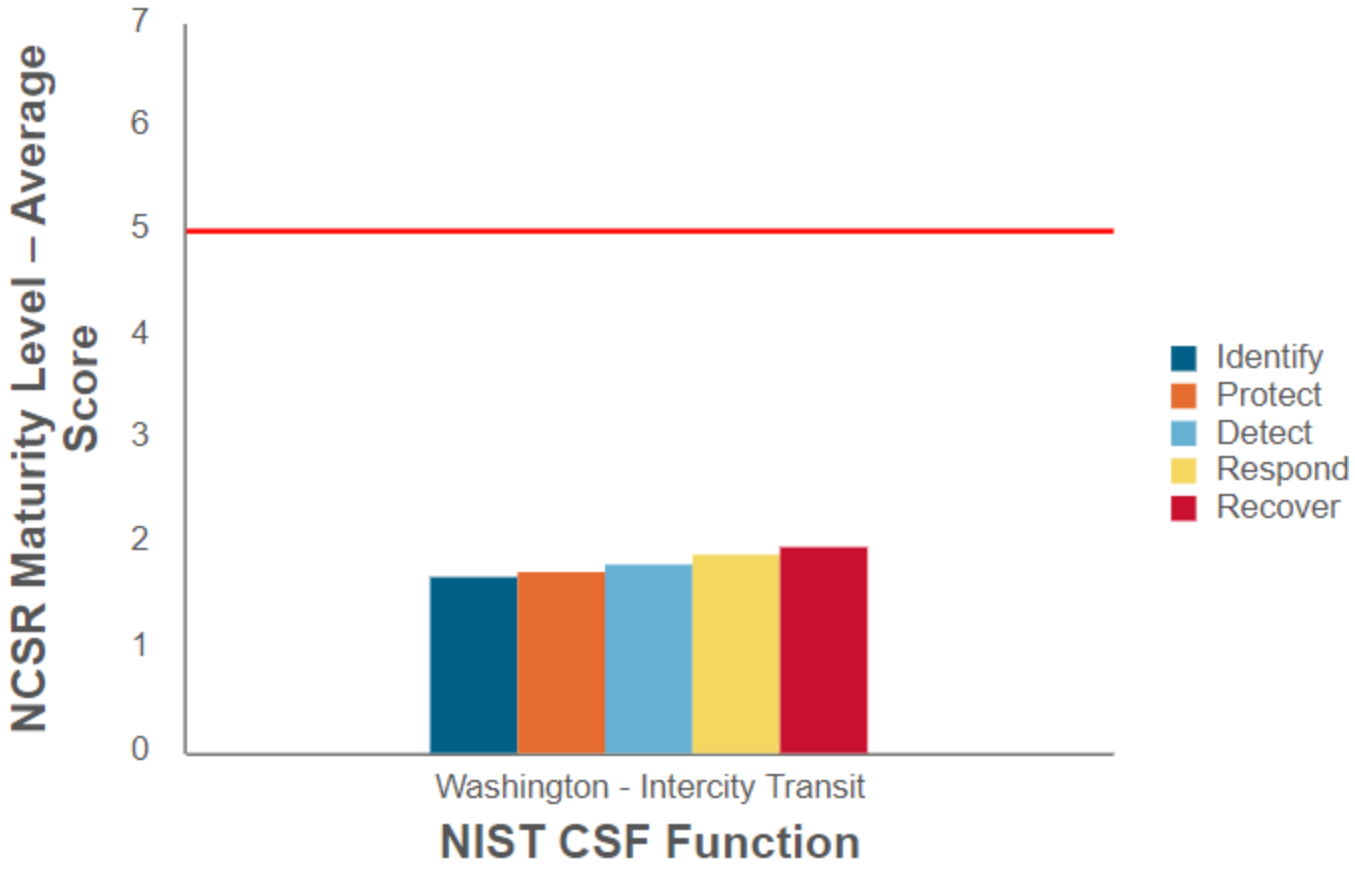
Outside cybersecurity experts

- NCSR (Nationwide Cybersecurity Review)
  - Sponsored by CISA, focused on state and local agencies
  - Based on the *Cybersecurity Framework* from the *National Institute of Standards and Technology* (NIST CSF)
- Aon CyQu (Cyber Quotient Evaluation)
  - Leading cybersecurity risk management company
  - Engagement coordinated through WSTIP

AON
Empower Results®

INTERcity TRANSIT

NCSR Result: 1.8/7



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

7	Optimized	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy	Your organization has a formal policy in place that has been approved by senior management.
2	Informally Done	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.
1	Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.

2021-04-25

CYBER HYGIENE

REPORT CARD

Intercity Transit, WA

2 Hosts with unsupported software

1 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

CISA CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

April 22, 2021 – April 25, 2021
Host Scans on All Addresses

April 22, 2021 – April 25, 2021
Vulnerability Scans on All Hosts

ADDRESSES OWNED

[redacted]
No Change

ADDRESSES SCANNED

[redacted]
No Change
100% of addresses scanned

HOSTS

[redacted]
No Change

SERVICES

[redacted]
No Change

VULNERABLE HOSTS

10
No Change
59% of hosts vulnerable

VULNERABILITIES

76
No Change

VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

INTERcity TRANSIT

2023-04-22

CYBER HYGIENE

REPORT CARD

Intercity Transit, WA

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

CISA CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

February 1, 2023 – April 22, 2023
Host Scans on All Addresses

April 19, 2023 – April 22, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

[redacted]
No Change

ADDRESSES SCANNED

[redacted]
No Change
100% of addresses scanned

HOSTS

[redacted]
No Change

SERVICES

[redacted]
No Change

VULNERABLE HOSTS

0
No Change
0% of hosts vulnerable

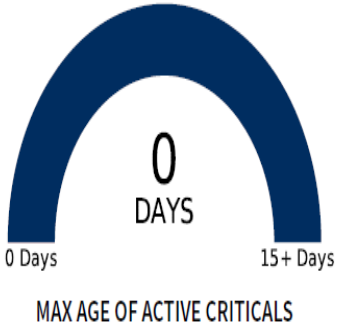
VULNERABILITIES

0
No Change

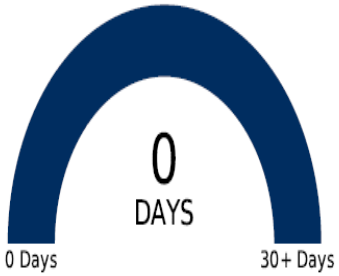
VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

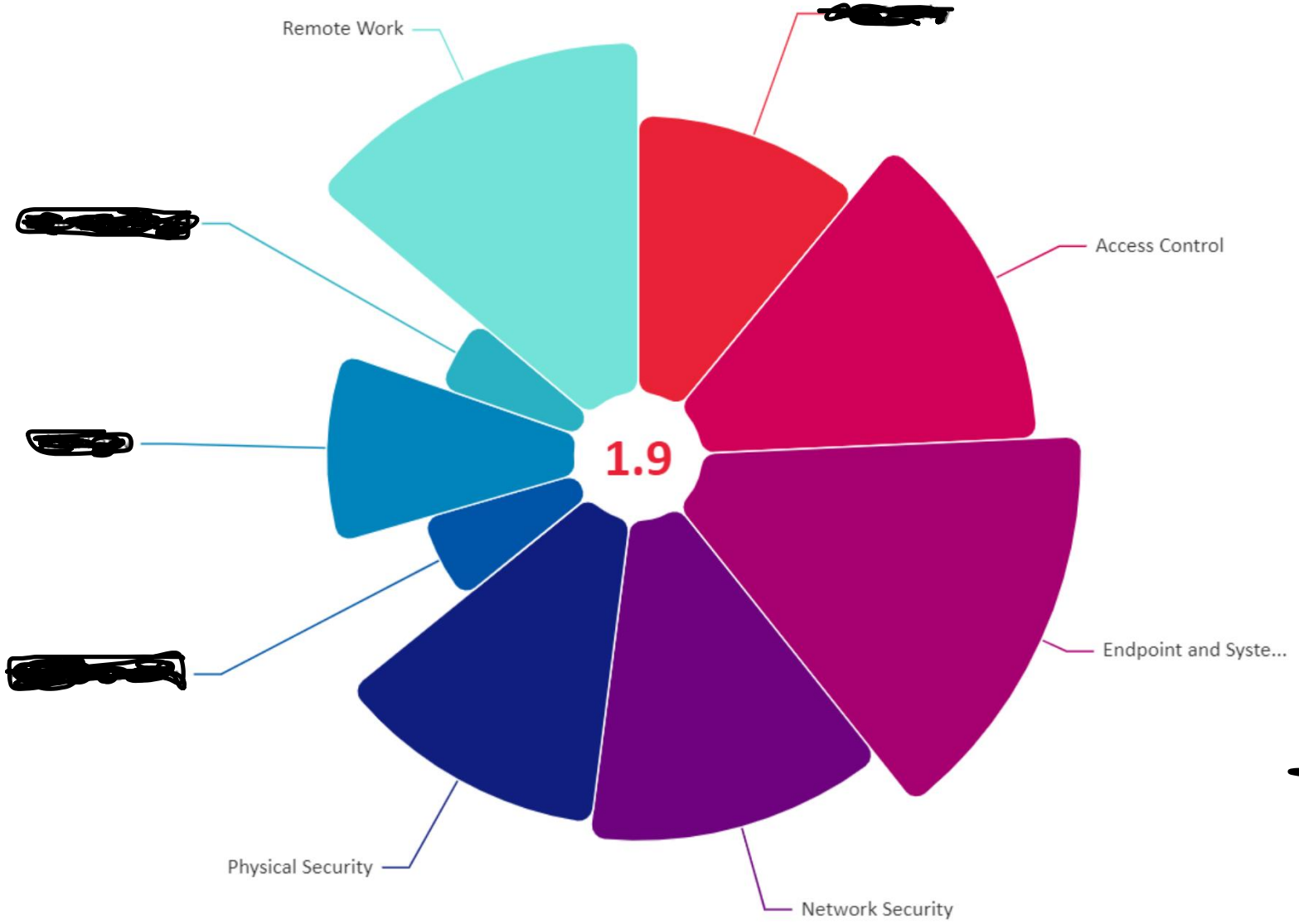
Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

INTERcity TRANSIT

WSTIP Pilot Agency

INTERcity TRANSIT

CyQu Result: 1.9/4



Results Key Index

0 - 1.9	Control not in place to manage the threat
2 - 2.5	Control is partially managing the threat
2.6 - 3.4	Control is currently managing the threat for most systems
3.5 - 4	Control is currently effectively managing the threat

[redacted]

1.9

ACCESS CONTROL

2.3

ENDPOINT AND SYSTEMS SECURITY

2.6

NETWORK SECURITY

2.2

PHYSICAL SECURITY

2.1

[redacted]

1.1

[redacted]

1.7

[redacted]

1.0

REMOTE WORK

2.4

Analysis of evaluations

- NCSR
  - We cannot score higher than 2 in any area without an organizationally adopted cybersecurity plan and dependent policies.
  - This masks the effect of best effort work done informally by IS staff to secure our infrastructure.
- Aon CyQu
  - Focus on avoiding risk and preparation to responding to incidents
  - We cannot adequately prepare to respond to incidents without an organizationally adopted cybersecurity plan.

New Policy Encacted! (PTACP)

MISSION STATEMENT

Cybersecurity is a core business function of Intercity Transit ("the agency"). The agency must protect the ***confidentiality, integrity, and availability*** of its information systems to support continuous safe and reliable operation of critical transportation infrastructure and foster a culture of trust and accountability inside and outside the agency. Starting with the General Manager, all employees are collectively responsible for the agency's cyber hygiene and the success of its cyber defenses. This Public Transportation Agency Cybersecurity Plan formalizes the agency's commitment to:

- Regularly assess and actively manage cybersecurity risks
- Comply with legal and regulatory cybersecurity and privacy requirements
- Strategically implement cybersecurity best practices recognized by government and industry
- Provide adequate skilled workers and resource allocation to execute this plan
- Promote employee cybersecurity awareness through regular training and communication
- Integrate cybersecurity into the job responsibilities of all employees
- Hold each employee accountable for secure and appropriate use of information systems
- Monitor information systems for vulnerabilities and indicators of compromise
- Identify and respond to cybersecurity incidents and report breaches
- Continually improve cybersecurity posture through management processes that enforce policies and measure their effectiveness
- Ensure vendor supply chains meet industry-recognized cybersecurity best practices

I hereby enact this Public Transportation Agency Cybersecurity Plan.

Ann Freeman Manzanares
Ann Freeman-Manzanares, General Manager

2/15/2023
Date

INTERcity TRANSIT

New Policy Encacted! (PTACP)

DOCUMENT HISTORY

- 2021-03-05 Information Management Policy draft (2021.1) created by Shem Sargent, Intercity Transit Information Systems Security Analyst.
- 2021-04-23 First Draft (2021.1) completed by Shem Sargent.
- 2021-05-10 Second Draft (2022.2) completed by Shem Sargent.
- 2021-05-17 Draft policy submitted to **SMT**.
- 2021-07-27 Third draft (2021.3) started by Shem Sargent. Remodeling document to align with form and intent of similar FTA Public Transportation Agency Safety Plan (PTASP, 49 CFR 673).
- 2022-03-08 Fourth draft (2021.4) started by Shem Sargent to add KPIs and superseded agency policies sections.
- 2022-04-12 Replaced Category 3 guidance with reference to agency Public Records Exclusion Key.
- 2022-04-15 Fourth draft completed by Shem Sargent. Edits finalized for legal review. Version number changed to 2022.1
- 2022-05-23 Legal review and edits completed by Jeffrey S. Myers of Law, Lyman, Daniel, Kamerrer & Bogdanovich, P.S.
- 2022-06-01 Version 2022.1 incorporating legal review completed by Shem Sargent and submitted to **SMT** for review.
- 2023-01-19 **SMT** review completed, and comments returned for revision.
- 2023-01-20 Version incremented to 2023.1; revision started by Shem Sargent, Cybersecurity Program Manager, and Jason Aguero, **CIO**
- 2023-02-13 Final review with **CIO** and delegated members of **SMT**. Version incremented to 2023.2

INTERcity TRANSIT

Table Top Exercise

- Conducted in March 2023
- On-site facilitation by the Department of Homeland Security
- Focus was on response and process identification during a simulated cyber incident
- Third part observer for feedback – Cybersecurity Experts
- Next steps – In Process

What's Next

INTERcity TRANSIT

Questions?