TRANSPORTATION & PUBLIC WORKS COMMITTEE

December 11, 2023
9:30 A.M.
Virtual Meeting

MINUTES

1. WELCOME AND INTRODUCTIONS

Mr. Chris Letnaunchyn, Chair, opened the meeting; attendees introduced themselves.

2. COMMENTS ON NOTES FROM SEPTEMBER 11, 2023, MEETING

There were no comments on the minutes.

3. INTEREST IN CYBER RESILIENCE REVIEW OF SIGNAL SYSTEMS/TRAFFIC MANAGEMENT SYSTEMS

Mr. Jason Schaum (Supervisory Cybersecurity Advisor (Maryland) – Region III Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security) provided an overview of cyber resilience reviews (CRR) and cyber assessments offered by CISA. CISA has various assessments that they offer aimed at different levels of staff.

The CRR is aimed at top level management and provides strategic feedback with recommendations for processes, procedures, and policies that would be undertaken over the months/years. The CRR offers input on how resilient the system is to continue operating in the event of a major cyber incident.

The Cybersecurity Performance Goals assessment would be at the tactical level and provide a baseline of cyber defensive capability.

Technical assessments would identify actions that should be taken in days/weeks timeframe.

Most of the assessment forms that CISA uses are in the Cybersecurity Evaluation Tool available online (https://www.cisa.gov/downloading-and-installing-cset).

Another offering from CISA is Cross Sector Cyber Performance Goals assessment (https://www.cisa.gov/cpg) which is shorter (several hours) than the CRR, covering 38 cybersecurity practices for information technology and operational technology systems.

The CRR has 299 questions that are derived from the Carnegie Mellon University CERT Resilience Management Model. The CRR evaluates the maturity of an organization's capacities and capabilities across 10 domains:

- Asset Management: all assets including technologies, people and data
- Controls Management: what controls are in place
- Configuration and Change Management: what configuration and change management processes are in place
- Vulnerability Management: what is the vulnerability management process; how to become aware of and mitigate vulnerabilities
- Incident Management: what is the incident management process and plan
- Service Continuity Management
- Risk Management
- External Dependencies Management: focused primarily on vendor relationships or other third parties supporting your service
- Training and Awareness
- Situational Awareness

All data collected by CISA for any assessments is protected under the Protected Critical Infrastructure Information (PCII) Program; it is not subject to disclosure under freedom of information act requests, public disclosure laws, civil litigation requests, or for regulatory purposes. It was also noted by an attendee that this type of information is protected under Maryland law also.

Each CRR focuses on a selected Critical Service. The service of focus that we are considering is traffic control. The CRR would then focus on the assets and services of the critical service:

- People: i.e., administrators, technicians, incident response personnel
- Information: i.e., data, set points, configuration files
- Technology: i.e., servers and software, firewalls, PLCs
- Facilities: i.e., data centers, emergency operation center, remote equipment closets

The CRR produces a 100+ page report that includes various resources, including:

- Comparison data with other CRR participants
- Summary "snapshot" graphic related to the domains of the NIST Cyber Security Framework (Identify, Protect, Detect, Respond, and Recover).
- Details on existing domain performance and options for consideration

To get started, an agency needs to contact CISA to request a CRR (or any) assessment. The next steps are:

- Agency works with CISA to schedule CRR Pre-assessment call; CISA conducts pre-assessment call with stakeholders to identify assets
- CISA conducts CRR Assessment
- CISA prepares draft CRR report
- CISA delivers draft CRR report
- CISA provides debrief on the CRR report

- CISA delivers final CRR report

The process can be completed in several months.

In the last couple of years, some of the region's water systems worked with CISA to conduct CRRs. In the debrief process, staff from each facility were able to identify about three to six priorities with the highest impact.

Mr. Schaum is working with the Cyber Preparedness Unit at Maryland Department of Emergency Management on cybersecurity.

There was a comment to consider evacuation routes when evaluating cyber resilience.

If an agency would like to initiate a CRR, contact Mr. Schaum (jason.schaum@cisa.dhs.gov; 202-746-2811).

[Presentation: Cyber Resilience Review (CRR) and CISA Cyber Assessments Overview]

4. CYBER EVALUATION METHODOLOGY

Mr. John Contestabile and Mr. Israel Lopez, Skyline Technology Solutions, provided an overview of a methodology to conduct a cyber-evaluation for state DOT traffic management centers (TMCs). The evaluation started with the CISA CRR tool and customized it to apply specifically to departments of transportation.

Information Technology (IT) security for enterprise networks has developed as threats have emerged and evolved. However, the Operational Technology (OT) security, for field devices for example, has typically not kept pace. Field devices used to be on a separate network but more are being included in the enterprise network. Field devices are typically operated by maintenance/operations staff whereas the enterprise network is operated by the CIO/IT staff. The IT staff may not have the expertise to deal with the OT networks/devices. So there can be an administrative distance as well as connectedness/technical distance between IT and OT.

There are three type of networks that support transportation technologies: traffic networks, business networks, and external networks. Mr. Contestabile said that there needs to be more attention on cybersecurity of the traffic networks.

The methodology Skyline developed uses the function-neutral National Institutes of Technology (NIST) Cybersecurity Framework (CSF) v 1.1 as the guiding framework for conducting the assessments and incorporated other more specific documents: National Cooperative Highway Research Program (NCHRP) Project 03-127 "Cybersecurity of Traffic Management Systems"; NIST Security and Privacy Controls for Information Systems and Organizations, Special Publication (SP) 800-53 Revision 5 (Special Publication (SP) 800-53r5); and Federal Highway Administration's Technical Report on "Transportation Management Center IT Security."

Skyline uses the Privva survey tool and divides questions into OT assessment and IT assessment. The result includes a summary table for OT and IT findings for identified threats.

Based on the assessments from over a dozen state DOTs, the following typical transportation themes across both IT and OT were identified:

1. IT and OT Boundary Standard: related to the separation between IT and OT networks, is it consistent across DOT regions, for example.
2. Security Hygiene
3. Network Documentation
4. Network Services Architecture: is this consistently the same across an agency? Is the equipment the same? Is the network the same? This can be problematic across an agency trying to manage the network.
5. Identity Management, Passwords, and MFA: personnel training on this is very important.
6. Log Management, SIEM, and Time Servers
7. Governance: Policies and Procedures
8. Asset Inventory and Management
9. Personnel Training
10. Vulnerability Management: networks need to be scanned regularly for vulnerabilities
11. Email Security

Good cybersecurity practices include addressing issues related to people, process, and technology.

After the presentation, it was noted that the CISA CRR is a good place to start. The kind of work that Skyline does can help delve more deeply into identifying issues and help address the identified issues.

Today's DOTs have many different systems to support their infrastructure and cybersecurity operations are an increasingly important part of agency operations. Agencies are encouraged to begin a cybersecurity assessment to develop a baseline and identify issues to address.

[Presentation: DOT Traffic Management Centers: Cyber Security Assessment Methodology]

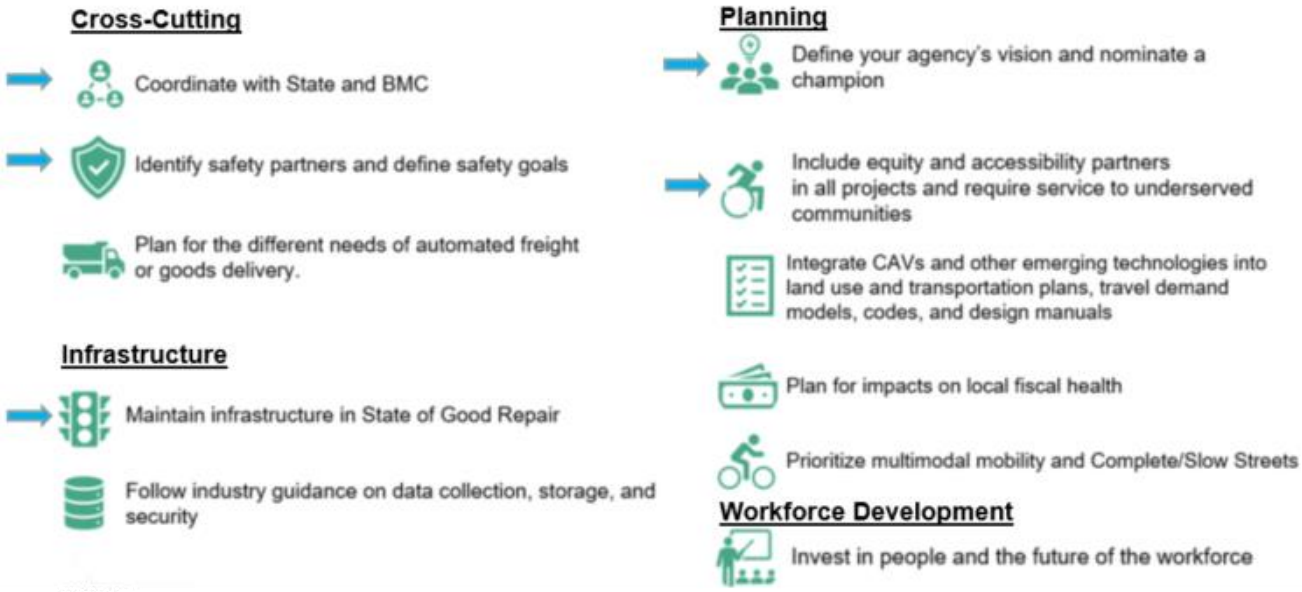
5. PREPARING FOR CONNECTED AND AUTOMATED VEHICLES

Ms. Singleton provided a short overview of the recently completed regional project on preparing for connected and automated vehicles (CAVs). The purpose of the project was to provide local jurisdictions and the region with recommendations for preparing for CAVs and to identify areas where local governments could incentivize and guide CAV deployments.

The project includes four parts:

- Literature review/White paper
  - Provides a concise resource for local jurisdictions on CAV technologies, role of local governments, challenges and benefits from CAVs, roles of different stakeholders, and examples of how other agencies are preparing for CAVs
- Customized recommendations for the region
  - The 11 recommendations are grouped into four areas: cross-cutting, infrastructure, planning, and workforce development

- The high priority areas identified by the project stakeholders address equity, safety, emergency response, built environment and infrastructure, collaboration, and community education. The recommendations are shown below, with the high priorities identified by a blue arrow:



- User Guide
  - Assists with working through the recommendations using a writable PDF
- Executive Summary

Ms. Singleton asked attendees if they would be interested in having a meeting to focus on walking through the User Guide. There was agreement that having a meeting would be beneficial. There was a suggestion to include representatives from the Maryland CAV Working Group and possibly the sub groups to provide input to the discussion.

[Presentation: Transportation & Public Works Committee, Notes for Agenda Items]

6. UPDATE ON RCPGP EVACUATION PROJECT

Ms. Singleton asked for thoughts to bring to the Evacuation TTX After Action Conference to be held December 12th. There was brief discussion about the role and future of the unified coordination group and the definition of "coordination" versus "command and control."

[Presentation: Transportation & Public Works Committee, Notes for Agenda Items]

7. COMMITTEE UPDATES

Disaster Debris Planning Task Force: At this time, it seems that local jurisdictions would likely not get reimbursed if using the state debris contracts (unless under exigent circumstances). Maryland DGS staff is in the process of preparing procurement documents for the next round of debris contracts and they are trying to structure them to meet FEMA procurement requirements for non-state entities.

[Presentation: Transportation & Public Works Committee, Notes for Agenda Items]

8. GROUP DISCUSSION

- The issue of reduced transportation budget was noted.
- Upcoming event: Ravens are playing in Baltimore City on New Year's Eve day at 1 PM.

[Presentation: Transportation & Public Works Committee, Notes for Agenda Items]

9. OTHER BUSINESS

- There is still interest in a discussion the issue of employee recruitment and retention.

2024 Meetings – March 11, June 10, September 9, December 9 (TBD if hybrid or remote)

ATTENDEES

Members

Azzam Ahmad, Baltimore City Dept. of Public Works
Bethany Brown, Maryland Dept. of Human Services
John Contestabile, Skyline
Bong Delrosario, Maryland Dept. of Disabilities
John Dulina, Maryland Dept. of Emergency Management
Eric Fogle, MDOT State Highway Administration OTMO
Kim Grove, Baltimore City Dept. of Public Works
Bill Johnson, MDOT State Highway Administration
Sam Kahl, Harford County Dept. of Public Works
Jeramy Lanning, MDOT State Highway Administration OTMO
David Larsen, Maryland Dept. of Transportation
Chris Letnaunchyn, Carroll County Dept. of Public Works
Timothy Peck, MDOT State Highway Administration
Mike Sheffer, MDOT State Highway Administration
Kris Singleton, Howard Co. Dept. of Public Works
Jim Small, Anne Arundel Co. Dept. of Public Works
Todd Tracey, MDOT Maryland Transit Administration OEM
Steve Walsh, Harford County Dept. of Public Works
Graham Young, Baltimore City Mayor's Office of Infrastructure Development

Staff and Guests

Israel Lopez, Skyline
Nicole Ramsey, Baltimore Metropolitan Council (BMC)
Jason Schaum, USDHS CISA
Eileen Singleton, BMC