Transportation Cybersecurity Incident Response and Management Framework

Cybersecurity Incident Exercise Summary Report

www.its.dot.gov/index.htm

Final Report—May 2021
FHWA-JPO-21-850

U.S. Department of Transportation

Produced by Southwest Research Institute under contract to
Cambridge Systematics, Inc. for the
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Federal Highway Administration
Intelligent Transportation Systems Joint Programs Office

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. FHWA-JPO-21-850	**2. Government Accession No.**		**3. Recipient's Catalog No.**
4. Title and Subtitle Transportation Cybersecurity Incident Response and Management Framework Cybersecurity Incident Exercise Summary Report			**5. Report Date** May 2021 **6. Performing Organization Code**
7. Author(s) Marisa C. Ramon and Austin T. Dodson.			**8. Performing Organization Report No.**
9. Performing Organization Name and Address Southwest Research Institute® (SwRI) 6220 Culebra Road San Antonio, TX. 78227 Under Contract to Cambridge Systematics Inc.			**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH61-16-D-00051
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Highway Administration Office of Operations (HOP) 1200 New Jersey Avenue, SE Washington, DC 20590			**13. Type of Report and Period Covered** Technical Memorandum December 2020—May 2021 **14. Sponsoring Agency Code** HOTM
15. Supplementary Notes The Contracting Officer's Representative is Joseph Gregory. We are grateful to Federal Highway Administration (FHWA's) stakeholder groups for providing their valuable comments.			
16. Abstract As part of the 2017 United States Department of Transportation (USDOT) Federal Highway Administration (FHWA) Roadway Surface Transportation Cybersecurity Framework project with Institute of Transportation Engineers (ITE), gaps were identified regarding the sharing of information amongst transportation stakeholders such as Infrastructure Owner Operators (IOOs) and municipal transportation agencies. FHWA now seeks to address some of these deficits by using previously improved procedures to conduct a cybersecurity incident exercise. As part of this process, this Incident Exercise Summary focuses on detailing the results of the completed Cyber Incident Exercise and using collected data to compare proposed protocols against traditional processes.			
17. Keywords Transportation, Cyber Resilience, Cybersecurity incident	**18. Distribution Statement** No restrictions.		
19. Security Classify. (of this report) Unclassified	**20. Security Classify. (of this page)** Unclassified	**21. No. of Pages** 44	**22. Price** N/A

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Acknowledgments

The authors wish to thank Ms. Erin Flanigan and Mr. Bruce Eisenhart for their direction and guidance on this document.

Table of Contents

Executive Summary 1

Chapter 1. Introduction 3

Background 3

Objective 3

Chapter 2. Cybersecurity Incident Exercise 5

Goals 5

Agenda 5

Exercise Details 6

The Scenario 9

Key findings 9

Differences in Score Due to Changes in Communication Process 9

Unanticipated Results from Observations of Participants Behaviors 10

Recommendation for Changes to Developed Processes Based on the Exercise 10

Lessons Learned 11

Chapter 3. Conclusion 13

Appendix A. Exercise 1 Results—Rubric 15

Appendix B. Exercise 2 Results—Rubric 21

Appendix C. Incident Exercise Chat Log 29

Participants 29

Exercise 1—First run of Cybersecurity Incident Exercise 29

Exercise 2—Second Run of Cybersecurity Incident Exercise 32

List of Tables

Table 1. Participants. 6

List of Figures

Figure 1. Flowchart. Proposed incident response process flow. 8

List of Acronyms

Acronym	Definition
AASHTO	American Association of State Highway and Transportation Officials
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DMS	Dynamic Message Sign
DOT	Department of Transportation
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FC	Fusion Center
FHWA	Federal Highway Administration
GM	Game Master
IMP	Incident Management Plan
IOO	Infrastructure Owner Operators
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organizations
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation System
LE	Law Enforcement
MS-ISAC	Multi State Information Sharing and Analysis Center
PIO	Public Information Officer
POC	Point of Contact
SME	Subject Matter Expert
SwRI	Southwest Research Institute
TLP	Traffic Light Protocol
TMC	Transportation Management Center
TOCOR	Task Order Contracting Officer’s Representative
USDOT	United States Department of Transportation

Executive Summary

As part of the 2017 United States Department of Transportation (USDOT) Federal Highway Administration (FHWA) Roadway Surface Transportation Cybersecurity Framework project with Institute of Transportation Engineers (ITE), gaps were identified regarding the sharing of information amongst transportation stakeholders such as Infrastructure Owner Operators (IOOs) and municipal transportation agencies. In order to address these deficits, communication protocols were developed and tested by conducting a cybersecurity incident exercise. As part of this process, this Incident Exercise Summary focuses on the following objectives:

- Detail the proceedings of the completed Cybersecurity Incident Exercise.
- Use collected data to compare the proposed protocols against traditional processes and comparing reach and speed of dissemination of information.

This exercise summary presents the proposed procedures and all collected data from the completed incident exercise, including the exercises performed and the participants involved. The cyber incident exercise was composed of two parts designed to assess the participants current understanding of information sharing and any improvements gained by following the proposed protocols. In the first part of the exercise, participants were expected to share information on the exercise based on their prior knowledge. Followed by participants receiving the proposed protocols and were asked to follow them when sharing information. Both parts include a staged active cyber-attack, with the difference being the presentation of the developed protocols to the participants in the second exercise.

Following a summary of these exercises, the actions of the participants are presented against the rubrics developed in the incident exercise plan. In the first exercise, without the protocols provided, the participants focused on protecting connected devices and equipment by disconnecting and implementing Information Technology (IT) response measures. After the first exercise, they were given the chance to review the developed protocols. The participants were more effective in communicating in terms of both speed and reach.

Summary of key takeaways are:

- Participants were able to more effectively share and disseminate cyber incident information using the developed protocols.
- Many of the participants (and the larger transportation community) are still unfamiliar with the information sharing resources available to them and will require pre-coordination prior to a real cyber incident.
- Participants focused on the recovery of devices and equipment affected by cyber incidents and postponed sharing vulnerability information with other departments and organizations.

The participants were also given the opportunity to discuss lessons learned. These lessons largely focused on the participants unfamiliarity with many of the resources available to them regarding

communication. The participants also expressed interest in reevaluating their current communication process to better match the presented protocol.

Given these findings, improvements were made to the Cybersecurity Incident Exercise process and more organizations can be informed on proper communication protocols.

Chapter 1. Introduction

Background

As part of the 2017 USDOT FHWA Roadway Surface Transportation Cybersecurity Framework project with ITE, research identified that gaps existed for vulnerability and exploit information sharing amongst IOO, Federal Bureau of Investigation (FBI)/Law Enforcement (LE), and Independent Security Researchers. Gaps included a deficit in communication pathways and willingness to share and receive cybersecurity threat intelligence as it relates to roadway transportation. FHWA seeks to reduce identified gaps by recommending process improvements to promote information sharing with transportation roadway stakeholders. As a part of this, SwRI developed recommended procedures to follow for potentially affected stakeholders in the case of vulnerability discovery, or a cyber-attack. These procedures were then tested using an example Cybersecurity Incident Exercise, the results of which are presented in this document.

Objective

The main purpose of this document is to cover lessons learned from the execution of the Cybersecurity Incident Exercise. Through reviewing activities from the exercise, the research team will be able to identify areas in which the developed cybersecurity incident communication protocols were successful or may need improvements. The following objectives have been identified for this Incident Exercise Summary:

- Detail the activities of the completed Cybersecurity Incident Exercise.
- Use collected data to compare the proposed protocols against traditional processes and comparing reach and speed of dissemination of information.

The document also identifies participants of the cyber incident exercise and key findings from each of the activities of the exercise. Through the successful completion and analysis of the exercise, the research team will gain valuable data about how individuals and organizations in the transportation sector share cybersecurity incident related information. This data will inform any needed protocol improvements and the activities of any future Cybersecurity Incident Exercises.

Chapter 2. Cybersecurity Incident Exercise

The following sections will go into detail concerning the cybersecurity incident exercise activities.

Goals

The goal of the Cybersecurity Incident Exercise was to compare the proposed cybersecurity communication process flow versus the traditional process used by participants. To achieve this goal, the research team established an Incident Exercise Plan detailing the execution of the exercise. This exercise included two main parts as shown below in the agenda activities. First was an incident exercise to be executed without providing the protocols developed. Next, another incident exercise was completed where the participants were provided with the recommended protocols. The comparison of the results of these exercises provides the data necessary to determine any improvements to the developed protocols.

Agenda

- Introduction—10 minutes
  - Participant and exercise introduction
- Conduct Exercise 1—60 minutes
  - Participants respond to the presented cyber incident with only prior knowledge
- Exercise 2 Introduction—30 minutes
  - Recommended communication protocol is provided to the participants with the opportunity to review
- Conduct Exercise 2—60 minutes
  - Participants respond to the presented cyber incident with the provided protocols
- Lessons Learned—20 minutes

The participants listed in table 1 are provided the opportunity to share any lessons learned through the incident exercise.

Table 1. Participants.

Name	Organization	Title
Phil Peevy	American Association of State Highway and Transportation Officials (AASHTO)/Georgia Department of Transportation (DOT)	AASHTO Fellow
John Thai	Anaheim DOT	Principal Traffic Engineer
Derek Arnson	Arizona DOT	Transportation Management Center (TMC) Manager
Mark DeLugt	Arizona DOT	Dispatch Manager
Ekaraj Phomsavath	FHWA	Intelligent Transportation System (ITS) Engineer
John McFadden	Tallahassee DOT	Transportation Management System Network Administrator
Joshua Hollingsworth	Tallahassee DOT	Traffic Engineer
Joe Gregory	FHWA	Task Order Contracting Officer's Representative (TOCOR)
Edward Fok	FHWA	Task Advisor
Ray Murphy	FHWA	Task Advisor
John Harding	FHWA	Task Advisor
Erin Flanigan	Cambridge Systematics	Task Project Manager
Marisa Ramon	SwRI	Lead Researcher
Cameron Mott	SwRI	Researcher
Austin Dodson	SwRI	Researcher
Josh Johnson	SwRI	Director
Victor Murray	SwRI	Manager

Exercise Details

To aid in the execution and quantitative assessment of the cyber incident exercise, the research team defined multiple concepts as follows:

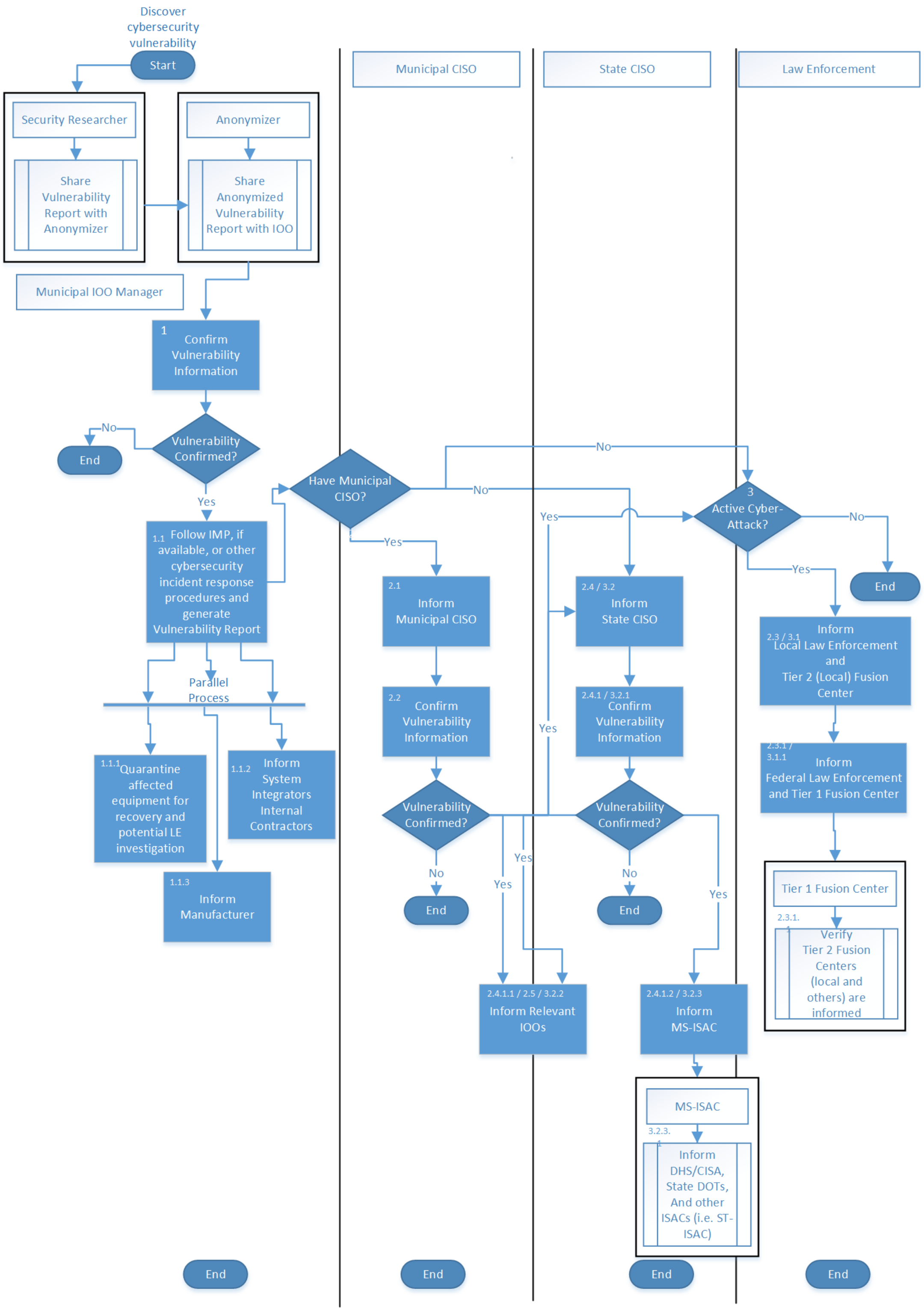
- Game Master (GM)—Leads the cyber incident exercise and prompts the participants with injects from the scenario (defined below). These injects may include statements like "An attacker has gained access to your network; how do you respond?".
    - Note: Other members of the research team may be called on by the GM for assistance (e.g., providing the participants with necessary materials during the execution of the cyber incident exercise).

- Scenario—The attack to be presented to participants during the cyber incident exercise. This often takes the form of injects to the participants from the GM.
- Role—The type of transportation stakeholder that a participant is assigned during execution of the cyber incident exercise. Example roles include:
  - Municipal IOO
  - State CISO
  - MS-ISAC/Other ISAC
- Action—The particular response of a participant during a turn (defined below). Actions taken by participants depend on both the assigned role of the participant and the current inject presented by the GM. These actions may include:
  - Implementing their incident management plan (IMP).
  - Sharing a vulnerability report with other participants (e.g., participant with the role of State CISO).
  - Contacting other participants with information on the cyber incident.
- Turn—The period in which participants may take an action in response to an inject from the GM. The end of a turn is marked when all participants have had the opportunity to take an action (*note: no action is also valid*).
- Points—Assigned according to the rubrics shown in Appendix B. Points assigned are considered based on both timing (in turns) and content of actions taken by participants. For example, higher points mean that a participant is sharing information effectively and in a timely manner, while lower points mean that a participant may not be sharing information (or not enough information, see vulnerability report sharing) or may not be sharing it in a timely manner.

Using these concepts, the basic flow of the exercise is as follows:

- GM presents the participants with injects from the established scenario, starting a new turn.
- Participants take actions according to their role during the turn.
- When all participants have had the opportunity to take an action, the turn is finished, and points are assigned based on the current turn and the content of the action taken.
- The GM then presents another inject, marking the start of another turn.

To test exercise participant communication aspects of cybersecurity incident response and examine the effectiveness of the proposed incident response process flows, the GM presented an attack in which an attacker uses a vulnerability to gain access to multiple TMCs’ dynamic message signs (DMSs). This scenario was presented twice, both with and without the proposed incident response process flows shown in figure 1.


Discover cybersecurity vulnerability
Start
Municipal CISO
State CISO
Law Enforcement
Security Researcher
Share Vulnerability Report with Anonymizer
Anonymizer
Share Anonymized Vulnerability Report with IOO
Municipal IOO Manager
1 Confirm Vulnerability Information
No
End
Vulnerability Confirmed?
Yes
1.1 Follow IMP, if available, or other cybersecurity incident response procedures and generate Vulnerability Report
Parallel Process
1.1.1 Quarantine affected equipment for recovery and potential LE investigation
1.1.2 Inform System Integrators Internal Contractors
1.1.3 Inform Manufacturer
Have Municipal CISO?
No
Yes
No
2.1 Inform Municipal CISO
2.2 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
Yes
Yes
2.4 / 3.2 Inform State CISO
2.4.1 / 3.2.1 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
Yes
2.4.1.1 / 2.5 / 3.2.2 Inform Relevant IOOs
2.4.1.2 / 3.2.3 Inform MS-ISAC
MS-ISAC
3.2.3.1 Inform DHS/CISA, State DOTs, And other ISACs (i.e. ST-ISAC)
3 Active Cyber-Attack?
No
End
Yes
2.3 / 3.1 Inform Local Law Enforcement and Tier 2 (Local) Fusion Center
2.3.1 / 3.1.1 Inform Federal Law Enforcement and Tier 1 Fusion Center
Tier 1 Fusion Center
2.3.1.1 Verify Tier 2 Fusion Centers (local and others) are informed
End
End
End
End

Source: FHWA

Figure 1. Flowchart. Proposed incident response process flow.

The Scenario

The attack begins when a security researcher notices a zero-day vulnerability in a common TMC software that results in bad remote access authentication certs. They also notice that a cyber threat actor has leveraged this vulnerability to execute a multi-state attack resulting in the attacker gaining access to the DMS remote control link in the various DOTs. The attacker then pushes a message update with an embedded attack that will wait until certain conditions (e.g., time, attacker-command) are met before executing over the remote-control link. The embedded attack executes simultaneously across TMC networks and begins to display false messages and locks the remote-control capabilities. Participants were then asked to respond and share information about the incident in a turn-based manner.

Key findings

This section summarizes the key findings from the execution of the cyber incident exercise.

Differences in Score Due to Changes in Communication Process

Through the first exercise of the Cyber Incident Exercise, the research team was able to discern what the participants knew and currently implemented within their TMC in terms of communication of cyber incidents. When faced with the cyber incident, many of the participants focused solely on response to the incident and how it would affect their equipment. This included:

- Attempting to remotely shut down equipment.
  - Met with an inject from the GM that the equipment was no longer able to be controlled remotely.
- Physically disconnecting effected equipment.
- Using cameras and other systems to verify where the attack on the equipment originated.

In the initial exercise, multiple turns passed in the game where information was either not being shared or not reaching all levels. Sharing as soon as information is received is key in these incidents as other TMCs may be affected or are being targeted by the attacker. At approximately six (6) turns into the first exercise, the participant playing the municipal IOO first shared information externally with their municipal Chief Information Security Officer (CISO) (opposed to one turn internally to TMC). As a result of the time it took participants to begin communication and the lack of some important sharing actions (e.g., share vulnerability report), the scores received by participants for this exercise were low. This exercise resulted in the following scores (full breakdown of the scores available in Appendix A):

- Municipal IOO—3 points
- Fusion Center (FC)/Multi State Information Sharing and Analysis Center (MS-ISAC)—1 point
- Municipal CISO—0 points
- State CISO—0 points

Following this initial exercise, the participants were provided the protocols developed by the research team. When using the protocols, there was still the initial concern of turning off effected devices but was instead completed in a single turn of “executing Incident Management Plan (IMP).” Without this focus, the participants communicated to outside organizations more quickly, with the first communication from the municipal IOO at around two turns instead of six turns like the first exercise. Many of the participants were able to improve their scores, resulting in the following (full breakdown of scores available in Appendix B):

- Municipal IOO—6 points
- FC/MS-ISAC—8 points
- State IOO—19 points
- Municipal CISO—0 points
- State CISO—0 points

As seen by the scores, participants following the developed protocols performed much better against the rubrics used in this exercise. They were able to share information more effectively and reach more individuals/organizations with that information. For example, the participant playing the municipal IOO role was able to begin communicating information at two turns opposed to their original six turns when following the proposed protocols.

Unanticipated Results from Observations of Participants Behaviors

Though the participants were able to more effectively share information, there were some instances where participants were unfamiliar with the other roles necessary for information sharing. For example, the participant playing the municipal IOO role was not sure if there was a Fusion Center in their area. The developed protocols assume that the actors have full knowledge of all resources available and do not take into account any pre-coordination that may be necessary (contacting Fusion center prior to a real cyber-attack for this specific example). This ultimately led to the municipal IOO not reaching out to the Fusion Center, and the municipal IOO not receiving points associated with contacting a Fusion center (lowering their overall score). This issue is solved by the participant conducting an outreach step, to be aware of potential resources at their disposal.

Also, participants often completed actions outside of the recommended path but reached a similar outcome. For instance, if a Municipal IOO was to contact their state CISO after contacting system integrators or contractors, there would be no score difference. In the developed protocols, it is recommended that municipal IOOs first contact their state CISO so that they contact organizations outside of the municipal IOOs reach. This change will need to be incorporated into the rubrics created, as this idea is reflected in the recommended protocols. Participants also did not take action to verify that attacks were taking place or that other organizations had come across the exploited vulnerability. In the proposed protocols, it is the state/municipal CISO’s responsibility to verify the information received from IOOs. Changes to the rubrics that score participant’s actions will need to be adapted to reflect this departure from the recommended protocol.

Recommendation for Changes to Developed Processes Based on the Exercise

Two recommendations for changes resulted from the execution of this exercise:

- Creation of an outreach step as a part of the developed processes, such that transportation stakeholders can identify all resources available to them and necessary to the developed processes prior to a cyber incident.

- Tuning of the scores assigned by the rubrics to prevent actions that, while they are necessary to the developed processes, are out of order and result in the same score as if a participant were to follow the processes exactly.

Lessons Learned

The participants were also asked to share any lessons learned through the exercise; responses are compiled below:

- Traffic Light Protocol (TLP)—Many of the participants were unfamiliar with the term, as there is a transportation-focused concept that shares the name. Transportation professionals and cyber security professionals need to be able to clearly distinguish between Traffic Light when referring to a traffic signal light, and Traffic Light Protocol when referring to cyber security intelligence information.
- Hesitancy to reach to Law Enforcement (LE)—Participant noted that they were hesitant to reach out because “we want absolute certainty. In the midst of all the chaos, we're likely not going to get that in the first few hours.” Their first priority is to close the connection to the TMC.
- Unfamiliarity with some of the roles discussed—Participants did not know they had Municipal CISOs or access to Fusion Centers.
- Reevaluation of current processes—Multiple participants stated that the exercise made them both question their current processes and express a desire to “reevaluate communication infrastructure, information dissemination protocols, and coordination in times of chaos.”

Chapter 3. Conclusion

To cover lessons learned from the execution of the Cyber Incident Exercise and analyze the effectiveness of the proposed cybersecurity incident response process flow, this incident exercise summary presents all data collected against the success criteria created in the incident exercise plan. The key findings from the Cyber Incident Exercise include:

- Participants were able to more effectively share and disseminate cyber incident information using the developed protocols.
- Many of the participants (and the larger transportation community) are still unfamiliar with the resources available to them and will require pre-coordination prior to a real cyber incident.
- Participants are often focused on devices and equipment affected by cyber incidents rather than sharing information with other organizations.

With this information, improvements can be made to the proposed cybersecurity incident response process flow and Cyber Incident Exercise. These improvements include:

- Creation of an outreach step as a part of the developed processes, such that transportation stakeholders can identify all resources available to them and necessary to the developed processes prior to a cyber incident.
- Tuning of the scores assigned by the rubrics to prevent actions that, while they are necessary to the developed processes, are out of order and result in the same score as if a participant were to follow the processes exactly.

These changes will address the main flaw identified by this cyber incident exercise and improve the effectiveness and repeatability of the proposed cybersecurity incident response process flow.

Appendix A. Exercise 1 Results—Rubric

The following are the rubrics used to assess the performance of participants during the first exercise. The "Action" column represents the action that a participant, acting in their role may take. Following the completion of any actions from participants, the GM will note that a "turn" has ended. The "Turn" column represents in which turn a given action was taken. The "Comments" column is for use by the GM, so that they can easily reference how many points may be assigned, based on which turn a participant completes an action. The "Points" column then represents how many points have been earned in a given exercise. In the case that a participant did not take a specific action, a '- is shown in the "Turn" column and no points were assigned.

In some instances, it is more beneficial to complete an action early (e.g., Municipal IOO—"Implement IMP") and a participant may receive less points for waiting to execute that action. Conversely, it is more beneficial to complete some actions later, and in the most extreme cases a participant may be docked points for completing an action too early (e.g., Municipal IOO—"Contact Equipment Manufacturer"). This scoring configuration helps reinforce that while the goal is to communicate in a timely manner, some actions should be taken first to ensure effectiveness of communication. For example, if a participant acting as a Municipal IOO first shares information with an equipment manufacturer, it is not guaranteed that the equipment manufacturer will share information with other affected IOOs or Information Sharing and Analysis Organizations (ISAO). In this example, the participant will be docked points for not beginning with their IMP or effectively communicating (e.g., reaching out to their CISO).

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Implement IMP	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Share Vulnerability Report with CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Special Case*: If IMP not implemented, Vulnerability Report generated and shared with Municipal/State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Contact State IOO	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Contact System Integrators/Contractors	3	1-2: -5 3-6: +3 points 8-12: +5 points 13+: +1 Never: 0	3
Other IOOs contacted	-	3-6: +3 points 8-12: +5 points 13+: +1 1-2: -5 Never: 0	-
Contact Equipment Manufacturer	-	4-7: +3 points 9-13: +5 points 14+: +1 1-3: -5 Never: 0	-
Contact Local LE[1]	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Contact MS-ISAC	-	4-7: +3 points 9-13: +5 points 14+: +1 1-3: -5 Never: 0	-
Vulnerability report includes: • Point of Contact (POC) of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using common vulnerability scoring system (CVSS) or similar	-	+5 for each bullet point included -5 for each bullet point missed	-

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • Common Vulnerabilities and Exposures (CVE) • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

[1] Unique to this scenario, LE many not be needed in other scenarios.

Fusion Center/MS-ISAC Rubric			
Action	**Turn**	**Comments**	**Points**
Inform LE	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Inform State IOOs/CISOs	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Inform other ISACs	1	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	1
Support provided to affected stakeholders	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-

Fusion Center/MS-ISAC Rubric			
Action	**Turn**	**Comments**	**Points**
Special Case*: Vulnerability discovered and report generated by ISAC (i.e., trend identification, spotting key performance indicators of large-scale impacts)	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-

Municipal CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Special Case*: If municipal CISO receives Vulnerability Report from municipal IOO Verify Vulnerability Report before sending to State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Contact State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the system integrator/contractor	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the equipment manufacturer	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Other IOOs contacted	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO contacts any ISAC	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-

Municipal CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Municipal CISO contacts LE or FC	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Vulnerability report includes: • POC of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using CVSS or similar	-	+5 for each bullet point included	-
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • CVE • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

Appendix B. Exercise 2 Results—Rubric

The following are the rubrics used to assess the performance of participants during the first exercise. See Appendix A for a description of the columns used.

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Implement IMP	1	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	5
Share Vulnerability Report with CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Special Case*: If IMP not implemented, Vulnerability Report generated and shared with Municipal/State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Contact State IOO	3	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	3
Contact System Integrators/Contractors	3	3-6: +3 points 8-12: +5 points 13+: +1 1-2: -5 Never: 0	3
Other IOOs were contacted	-	3-6: +3 points 8-12: +5 points 13+: +1 1-2: -5 Never: 0	-

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Contact Equipment Manufacturer	2	4-7: +3 points 9-13: +5 points 14+: +1 1-3: -5 Never: 0	-5[1]
Contact Local LE[2]	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Contact MS-ISAC	-	4-7: +3 points 9-13: +5 points 14+: +1 1-3: -51-21-3 Never: 0	-
Vulnerability report includes: • POC of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using CVSS or similar	-	+5 for each bullet point included -5 for each bullet point missed	-
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • CVE • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

[1] Note that -5 points were given from the individual taking an action too soon. Contacting the equipment manufacturer or an external source prior to confirming the vulnerability and contacting the managing Municipal/State CISO can adversely affect the efficacy of incident response handling.

[2] Unique to this scenario, LE many not be needed in other scenarios.

Fusion Center/MS-ISAC Rubric			
Action	**Turn**	**Comments**	**Points**
Inform LE	1	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	1
Inform State IOOs/CISOs	2	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	1
Inform other ISACs	4	1-3: +1 points 4-7: +3 points 7-10: +5 Never: 0	3
Support provided to affected stakeholders	5	1-3: +1 points 4-7: +3 points 7-10: +5 Never: 0	3
Special Case*: Vulnerability discovered and report generated by ISAC (i.e., trend identification, spotting key performance indicators of large-scale impacts)	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-

State IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Implement IMP	1	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	5
Special Case*: If State IOO receives Vulnerability Report from municipal IOO Verify Vulnerability Report before sending to State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-

State IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Contact State CISO	2	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	5
State IOO reports the vulnerability to the system integrator/contractor	2	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	3
State IOO reports the vulnerability to the equipment manufacturer	2	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	3
Other IOOs contacted	3	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	3
State IOO contacts any ISAC	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
State IOO contacts LE or FC	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Vulnerability report includes: • POC of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using CVSS or similar	-	+5 for each bullet point included	-

State IOO Rubric			
Action	**Turn**	**Comments**	**Points**
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • CVE • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

Municipal CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Special Case*: If municipal CISO receives Vulnerability Report from municipal IOO Verify Vulnerability Report before sending to State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Contact State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the system integrator/contractor	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the equipment manufacturer	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-

Municipal CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Other IOOs contacted	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO contacts any ISAC	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO contacts LE or FC	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Vulnerability report includes: • POC of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using CVSS or similar	-	+5 for each bullet point included	-
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • CVE • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

State CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Special Case*: If municipal CISO receives Vulnerability Report from municipal IOO Verify Vulnerability Report before sending to State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Contact State CISO	-	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the system integrator/contractor	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO reports the vulnerability to the equipment manufacturer	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Other IOOs contacted	1	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	3
Municipal CISO contacts any ISAC	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Municipal CISO contacts LE or FC	-	1-5: +1 points 6-10: +3 points 11-20: +5 Never: 0	-
Vulnerability report includes: • POC of reporting stakeholder • Description of the incident and audience designation, using TLP • Incident severity or level of impact using CVSS or similar	-	+5 for each bullet point included	-

State CISO Rubric			
Action	**Turn**	**Comments**	**Points**
Vulnerability report can be broken up into multiple reports based on TLP and could include additional information such as: • Equipment affected • Start/detection time • Status (such as ongoing/addressed/quarantined) • Planned next steps (NOT for TLP green or white distribution) • CVE • Role of POC • Direct/alternate contact method for POC	-	+1 for each bullet point included	-

Appendix C. Incident Exercise Chat Log

Participants

The following shows the roles taken by each participant for each of the exercises.

Role	Exercise 1	Exercise 2
Anonymizer	Phil Peevy	-
Municipal IOO	John McFadden	John McFadden
Municipal CISO	John Thai	John Thai
MS-ISAC/FC	Ekaraj Phomsavath	Ekaraj Phomsavath
State IOO	-	Mark DeLugt
State CISO	-	Phil Peevy

Exercise 1—First run of Cybersecurity Incident Exercise

The following are notes taken during the execution of the first incident exercise.

Turn 1.

a. Municipal IOO—Check out central system and see if anyone is on site

Turn 2.

a. Municipal IOO—Shutting off devices—furthest DMS is 20 min

Turn 3.

a. Municipal IOO—Communication with the state and other TMCs

i. Kill all connections to other TMCs

Turn 4.

a. Municipal CISO: Right now, it'd be coming to the field one DMS at a time or coming to a comm. hub to shut the others down.

b. MS-ISAC/FC: 12:06 PM—NJ FC provide situation awareness reporting.

c. Municipal IOO: 12:07 PM—Use central system to see if message came from TMC

d. Municipal CISO: 12:07 PM—However, with premeditation, one can shut down the entire attack within minutes from the TMC if properly designed.

e. Municipal IOO: 12:07 PM—Use cameras to see if anyone is at the DMS cabinet

f. MS-ISAC/FC: 12:08 PM—NJ Fusion center information sharing with cybersecurity division of State Office of Homeland Security

g. Municipal IOO: 12:08 PM—Share information with the regional TMC to see if they are having issues (as they have connectivity to our system)

h. Municipal IOO: 12:09 PM—Use Intelligent Transportation System (ITS) technicians to shutdown DMSs if messages cannot be blanked from TMC

i. Anonymizer: 12:09 PM—I would notify the lead agency being attacked, that they are under attack and from where in the system the attack is focusing

j. MS-ISAC/FC: 12:09 PM—Depending on the severity of the incident, FC will share the information with the FBI region office; cybersecurity Subject Matter Expert (SME)

    i. MS-ISAC/FC: 12:11 PM—NJ Fusion center SitRep reports are collated/compiled from State DOT TOC, State Office of Information Technology (OIT), MS-ISAC if any

    ii. MS-ISAC/FC: 12:12 PM—... need SMEs from either NJ State cybersecurity office or FBI region office to read log files for computer forensics

    iii. MS-ISAC/Fusion Center: 12:13 PM—SitRep reports are sent to anyone in the email distribution list consisting of State/local agencies dealing with emergency management, intelligence information sharing, etc.

Turn 5.

a. Municipal CISO: 12:12 PM—Bad VR? First step, shut down connection to either IT or Internet by physically removing the connections.

Turn 6.

a. Municipal CISO—Shut down all comms—2—from inside connect to all the signs and blank -3—visit all signs and shut down manually

b. Municipal IOO—once district knows about it, will not escalate

    i. Assume state knows about it

    ii. Get with city tech infrastructure administrator (CISO) and let her know

c. Municipal CISO—Vuln Report sharing: share with City Traffic Engineer, City Engineer first for guidance. Chances are we received the VR from IT so the IT head is already aware. Then wait for directions.

Turn 7. All IOOs have it, state has it, municipal CISO has it

a. Anonymizer: 12:21 PM—share with local law enforcement and DHS/CISA

    i. Anonymizer: 12:24 PM—any information I had on the attack and ask for a specific contact for future information

    ii. Essential info about the attack?

        - who conducted the attack.
        - where they attacked from if possible, what part of the system they attacked, how to close access to the attacker.

b. MS-ISAC/Fusion Center: 12:21 PM—State DOT/IT organizational unit office, State OIT, cybersecurity division of State Office of Homeland Security

c. Municipal IOO: 12:21 PM—Agencies to notify: City IT, FDOT District 3 TMC, FDOT Central Office

d. Municipal CISO: 12:22 PM—Supervisors will determine how to proceed with notifying Public Information Officer (PIO), law enforcement and IT and PW department. Chances are, the Emergency Operations Center (EOC) will soon be activated.

   i. Municipal CISO: 12:23 PM—We have over 20 DMS's so other PW field staff may assist in shutting down power to the signs if necessary.

   ii. Municipal CISO: 12:25 PM—I leave PIO and law enforcement to be liaison with FBI and the likes.

e. MS-ISAC/Fusion Center—FC coordinates with the FBI region offices in NJ (Newark) and PA (Philadelphia)

   i. Do you see interactions? Only authorized personnel of the FC are allowed to enter the intelligence operations room.

   ii. Will receive information through the fusion center—no direct interaction

Turn 8. Inject on equipment manufacturer

a. Municipal IOO: 12:26 PM—Getting with the manufacturer would be an action item to resolve the security issue. Resolving the threat would be the priority. Since we operate/maintain the DMSs, we'd have them offline till the issue was resolved and the manufacturer had a fix. The manufacturer is not local.

b. Municipal CISO: 12:27 PM—I would follow up with the manufacturer after the threat is gone. Threat connectivity is first priority.

Turn 9. Difference provided info between FC and MS-ISAC

a. Municipal CISO: 12:28 PM—That is above my pay grade.

   i. Next person up (who to contact)—Municipal CISO: 12:29 PM—Typically PIO or designee.

b. MS-ISAC/Fusion Center: 12:28 PM—State OIT normally interface with MS-ISAC; not the State DOT due to the organizational/command structure in the state

c. Municipal IOO: 12:29 PM—I have not had to coordinate with MS-ISAC or a fusion center, but I'd assume the City's network administrator or District's network administrator would have those connections

Turn 10. what point do you communicate to other IOOs?

a. Municipal CISO: 12:31 PM—mid process

   i. certain things that you would need to be aware of before?

   ii. Need authorization to reach out. Need good understanding of issues and certitude of data.

b. Municipal IOO: 12:31 PM—It would be early/mid once we found out how widespread the issue was.

   i. As soon as something was out of the ordinary and we did not have the control, they'd be notified ASAP

c. MS-ISAC/FC: 12:31 PM—as early as possible, and then more info. will be forthcoming for everyone's situational awareness

Exercise 2—Second Run of Cybersecurity Incident Exercise

The following are notes taken during the execution of the second incident exercise following training of proposed communication protocols and procedures.

Turn 1. Assume information from Anonymizer has been to send to all participants.

a. State CISO: 1:17 PM—1st—Contact internal IT and contractors responsible for the software. then execute the state incident management plan. notify local road agencies and law enforcement that the signs are down.

   i. Does everyone have an IMP? NJ perspective—traffic incident management plan, emergency management plan—no cyber incident management plan

b. State IOO: 1:14 PM—Notify technical staff and PIO's for public/social media dissemination, also notify affect cities/entities affected; that's it for my group

   i. State IOO: 1:23 PM—We have a PIO on duty in the TOC 24x7, our PIO Office have an extensive community outreach, we advise of the situation and they can do a timely, high-profile dissemination to the public

   ii. What information included and what would the role be?

   iii. State IOO: 1:24 PM—Administrative being the upper admin of the organization, to prepare them for the avalanche of question

   iv. State IOO: 1:25 PM—Upper management working with upper management Communications specialists

c. Municipal IOO: 1:18 PM—Contact Regional TMC and internal IT to notify of incident. We do not have an IMP (as far as I know)

   i. Municipal IOO: 1:19 PM—From the Municipal IOO perspective, we would leave the IMP implementation to the State DOT or internal IT

d. Municipal CISO: 1:25 PM—I think what Mark said applies to all staff levels

Turn 2. Confirming vuln—IMP being executed—

a. State CISO: 1:28 PM—develop and share vulnerability report with IT and contractors/manufacturer. Contact state CISO/CIO with report

   i. difference? That is a possibility

b. Municipal CISO: 1:29 PM—Have a chat with everyone for lessons learned, what went right/what went wrong and how to prevent future attacks.

   i. who is involved?

   ii. Municipal CISO: 1:31 PM—Start with IT who first announces vulnerability, then to TMC operators, then management, then law enforcement then PIO

c. Municipal IOO: 1:32 PM—Once issue has been mitigated, upper management would be notified of incident to deal with communications to the public. The vendor would be contacted for a patch. An internal meeting would happen with operators, maintenance staff, and internal IT to mitigate the issue from happening again

   i. Municipal IOO: 1:32 PM—The state DOT would be heavily involved in find what the issue was since they are the owners of all state infrastructure

d. State IOO: 1:32 PM—If the situation is still dynamic, keep updates going to all levels; once static and not resolved ensure backup plans are activated

e. MS-ISAC/Fusion Center: 1:33 PM—Fusion center will delegate it to the Cybersecurity division of the State Office of Homeland Security to send an advisory based on info. from State CISO.

Turn 3. —inject—FBI agent calls State CISO

a. State IOO: 1:34 PM—That would be an immediate transfer to the technical manager

b. Municipal CISO: 1:36 PM—When, where was the breach? At what level of breach? Is it still going on?

c. MS-ISAC/Fusion Center: 1:36 PM—... just to clarify the cybersecurity advisory would be based on info. from the State CISO, State DOT, State OIT, etc.

d. Municipal IOO: 1:37 PM—We would have to provide any answers that follow the public information request guidelines

Turn 4. —inject reach out to FC

a. Municipal IOO: 1:39 PM—No fusion center in my area (that I know of)

b. MS-ISAC/Fusion Center: 1:40 PM—... continue to feed the beast (Fusion Center) with info.

c. Municipal CISO: 1:40 PM—I personally am a bit leery of fusion centers

i. Municipal CISO: 1:41 PM—How are my data "fused?" Are my data compromised or misinterpreted? What vulnerability is possible with people going into my system?

ii. Municipal CISO: 1:42 PM—Are my (potentially misrepresented) data passed to the media and others?

d. MS-ISAC/Fusion Center: 1:45 PM—... due to established relationship, State OIT normally coordinates with MS-ISAC

i. MS-ISAC/Fusion Center: 1:46 PM—.. information flow from MS-ISAC to State OIT then will be share with Fusion Center; yes and it depends

Turn 5. —inject—inside actor at equipment manufacturer—interfering with updates

a. How to put together dissemination of info with access control labels?

i. Municipal IOO—municipal level would ask manager and leave it to the State DOT to handle

ii. MS-ISAC/Fusion Center: 1:52 PM—State cyber office used a template. The cyber security advisory will normally contain an overview, the scope of the incident, threat intelligence, systems affected, risks to businesses/governments, tech summary, references from U.S. CERT if any.

iii. State CISO: 1:52 PM—I would not communicate with any agency that did not have full access. I would coordinate with our Communication Office for any external information

U.S. Department of Transportation
ITS Joint Program Office—HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-21-850

U.S. Department of Transportation