Transportation Cybersecurity Incident Response and Management Framework

Final Report

www.its.dot.gov/index.htm

Final Report—July 2021
FHWA-JPO-21-851

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-21-851

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Transportation Cybersecurity Incident Response and Management Framework

Final Report

5. Report Date

July 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)
Mail Stop: E86-205
1200 New Jersey Avenue, SE
Washington, DC 20590

13. Type of Report and Period Covered

Final Report
January 2021—June 2021

14. Sponsoring Agency Code

HOTM

15. Supplementary Notes

The Contracting Officer's Representative is Joseph Gregory. We are grateful to 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), research identified that gaps existed for vulnerability and exploit information sharing amongst transportation stakeholders. These gaps included a deficit in communication pathways and willingness to exchange cybersecurity threat intelligence as it relates to roadway transportation. FHWA now seeks to reduce identified gaps by establishing processes to promote information sharing and developing a framework for communication and information sharing with transportation roadway stakeholders. To this effort, this Final Report's objective is to summarize the findings of this project effort.

17. Key Words

Transportation, Cyber Resilience, Cyber Incident

18. Distribution Statement

No restrictions.

19. Security Classif. (of this report)

Unclassified

20. Security Classif. (of this page)

Unclassified

21. No. of Pages

196

22. Price

N/A

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 project.

The authors also wish to thank the Kentucky Fusion Center, MS-ISAC, Steve Johnson, Susan Klasen, Josh Hollingsworth, Jeff Rockower, Adam Moser, Alejandro Motta, Crystal King, and Texas Department of Transportation (TxDOT) who took part in this solicitation effort and provided their valuable experiences regarding cyber-terminology improvements and input regarding cyber incident information sharing.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Definition
AASHTO	American Association of State Highway Transportation Officials
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FHWA	Federal Highway Administration
IMP	Incident Management Plan
IOO	Infrastructure Owner Operators
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ITE	Institute of Transportation Engineers
LE	Law enforcement
MCAP	Malicious Code Analysis Platform
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
N-DEx	National Data Exchange
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
PII	Personally Identifiable Information
PT-ISAC	Public Transportation Information Sharing and Analysis Center
SME	Subject Matter Expert
SOC	Security Operations Center
ST-ISAC	Surface-Transportation Information Sharing and Analysis Center
TLP	Traffic Light Protocol
U.S.-CERT	United States Cyber Emergency Response Team
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
USDOT	United States Department of Transportation

Executive Summary

Research conducted, 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), identifies existing gaps for vulnerability and exploit information sharing amongst transportation Infrastructure Owner Operators (IOOs), equipment manufacturers that supply IOOs, Law Enforcement (LE), and independent security researchers. These gaps limit communication and delay sharing of cybersecurity threat intelligence related to roadway transportation systems. The objective of this project was to address communication issues between transportation roadway stakeholders by identifying process improvements to improve transportation resiliency during a cyber incident. To this effort, this Final Report presents the findings of the "Transportation Cybersecurity Incident Response and Management Framework" project with regards to recommended improvements in procedures and processes for communication and information sharing prior to and during a cyber incident.

This project examined the existing gaps discovered during 2017 USDOT FHWA project, and resulting in a description of the problems, challenges, and opportunities stakeholders identified and a definition of needed actions to promote a culture of transportation system cyber resilience and improve information sharing. To understand the current information exchange landscape and determine improvements in information sharing, existing Information Sharing and Analysis Organization (ISAOs) were researched. Research focused on how ISAOs are used for information sharing and if there are any gaps in existing guidance that do not address transportation infrastructure requirements. With the current information exchange landscape identified, research then determined the data requirements required to provide the minimum information needed to assist stakeholders in cyber incident information exchange. Combining the information gained from the findings regarding the current information exchange landscape and the minimum requirements to provide a solution, research developed proposed improvements. The proposed improvements include transportation-centric cybersecurity terminology to aid in establishing their consistent usage and a cybersecurity incident communication process to improve the reach and speed of information dissemination during a cybersecurity incident event.

The following key results were derived over the course of this project and are described further in this report:

- Identification of the problems, challenges, and opportunities related to improving the speed of information distribution in the transportation community, as solicited from transportation stakeholders' inputs.
- Recommendations that address the need for culture and process improvements to cybersecurity information sharing that were developed based on input from these transportation stakeholders.
- Information to help identify and effectively utilize existing ISAOs such as Information Sharing and Analysis Centers (ISACs), Cybersecurity and Infrastructure Security Agency (CISA), Fusion Centers, and Emergency Operation Centers. This effort also identified minimum data requirements needed to effectively aid in understanding a cyber-attacks occurrence and a recommended information flow for effective cyber incident information exchange.

- Proposed common terminologies to unify across the transportation and cyber security community to improve understanding and conversations related to transportation cyber incident information sharing. This effort resulted in a cross-discipline glossary of terms (shown in Appendix C) to be used by both transportation and cybersecurity professionals when discussing transportation-related cyber incidents.
- Identification of improvements to procedures and processes for communication and information sharing prior to and during a cyber incident. These improvements are in the form of recommended process flows (shown in Appendix A) that demonstrate how a particular transportation stakeholder (e.g., Municipal IOO) can report information when faced with a cyber incident. These procedures were then tested in a Cyber Incident Exercise which presents a group of transportation stakeholders with a simulated cyber incident. This exercise demonstrated that the developed procedures helped to improve metrics such as cyber incident response time and content of information shared. Also, lessons learned and any improvements to the processes were captured during this effort.

In deriving these key results, the research team was able to clarify existing gaps and identify additional gaps in information sharing and develop improvements and supporting documentation to assist during transportation cybersecurity incident response and information sharing events. These improvements are discussed further in this Final Report and detailed information supporting the key results can found in the Appendices.

Chapter 1. Introduction

Project 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 IOOs, equipment manufacturers that supply IOOs, Federal and local 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.

Project Objective

The objective of this project was to develop a framework for communication and information sharing with transportation roadway stakeholders when detecting and responding to a cyber-attack or vulnerability that spans across devices common in transportation applications or other adjacent Department of Homeland Security (DHS) critical sectors (e.g., Energy, Information Technology). This project supported a cyber incident response exercise, which took a similar approach to a DHS "Cyber-Storm" exercise.[1] This included developing protocols and procedures for interfacing with ISACs and organizations like the National Cybersecurity and Communications Integration Center (NCCIC). By testing these protocols in a cyber incident response exercise, improvements to the protocols were extracted from lessons learned documented during the execution of the exercise.

The tasks performed as part of this project support the following:

- Conduct a Literature Review and Existing Resources.
- Define Transportation Infrastructure ISAC Requirements.
- Develop strategies to establish consistent usage of cybersecurity terminology, including a glossary.
- Identify ISAOs.
- Develop/Adapt Cybersecurity Incident Communication Protocols.
- Conduct Cybersecurity Incident Exercise and Refine Cybersecurity Incident Communication Protocols.

[1] https://www.cisa.gov/cyber-storm-securing-cyber-space

Chapter 2. Problem and Need

This research follows the 2017 USDOT FHWA project that solicited input from transportation stakeholders and identified that gaps existed for vulnerability and exploit information sharing. The following transportation stakeholder groups were interviewed separately to collect open and honest discussions on their experiences in sharing and implementing cyber security information:

- Public agencies, IOOs from National Association of City Transportation Officials (NACTO), Intelligent Transportation Society of America (ITS America), American Association of State Highway Transportation Officials (AASHTO).
- Equipment manufacturers and system integrators were represented by National Electrical Manufacturer Association (NEMA) and equipment manufacturers that supply IOOs.
- LE and national/state information reporting agencies represented by Federal Bureau of Investigation (FBI), DHS, and State Fusion Centers (FC).
- Security research communities.

Identified gaps pointed at the problems, challenges, and opportunities hindering communication and disrupting the speed of information distribution in the transportation community. These gaps highlighted the need for several actions that can be implemented to improve the speed and breadth of communication.

The following sections discuss these needed actions and describe the problems, challenges, and opportunities stakeholders identified to merit the recommended action. These actions are not listed in order of priority.

Culture Changes Needed for Transportation System Cyber Resilience

There are little to no incentives to changes in behavior except in cases where an IOO or equipment manufacturer has taken the additional steps to assess their vulnerability to cyber risks. Not all identified gaps and needs are solvable as a communication issue, some will require changes in behaviors. These conclusions were either gathered from interviews with stakeholders or derived by FHWA staff to address stakeholder concerns.

The following are findings received from the Stakeholders regarding the culture for transportation system cyber resilience:

- There was consensus from the Stakeholders that improvement in transportation system cyber resilience is needed.
- Patch management for most contemporary traffic control field devices does not exist.

- Cost minimization is the main driver for local operating agencies. There is little to no resources to do anything without external incentive or pressure.
- Part of the urgency is that transportation networks are interconnected, and exploits developed in low criticality jurisdiction could be weaponized at high criticality targets.

Cybersecurity Information Sharing Gaps Between Transportation Stakeholders

Below are identified gaps for information sharing regarding cybersecurity risks and vulnerabilities between IOO's, equipment manufacturers, law enforcement, and independent security researchers.

The following findings pertain to the existing communication protocol between IOOs/transportation stakeholders and equipment manufacturers:

- Communication between equipment manufacturers and IOOs is often not direct. Operational equipment is frequently provided to the customer through contractors, distributors, and other intermediate agents. This layer of separation frequently interrupts the two-way flow of information.
- Equipment manufacturers typically do not have established procedures to handle unsolicited reports from security researchers. Security researchers have mixed experiences with reporting to equipment manufacturers in this domain and frequently report directly to ISAC, ISAO, or Industrial Control Systems Computer Emergency Response Team (ICS-CERT).
- There is no clear visibility into the vulnerability communication in these organizations beyond some cases we are familiar with involving ICS-CERT.
- Manufacturers report that it may take a long time for patches to be disseminated to all devices in an organization. Safety related patches (e.g., patches that have implications to safety) have the highest priority. Cyber security patches are less common and not as high a priority.
- IOO's consider vulnerabilities as a problem the equipment manufacturers should address and expect that equipment manufacturers will take ownership if any problem occurs.

The following findings pertain to the communication protocol between IOOs/transportation stakeholders and law enforcement:

- Law Enforcement, NCCIC, and ISAO need access to domain subject matter experts (SMEs) to evaluate vulnerability information.
- An anonymous tip system is needed to encourage the reporting of discovered vulnerabilities.
- LE needs access to SMEs and equipment manufacturer response, possibly on short notice in response to incidents. This can be challenging since the initial assessment could include controlled access to (classified) information.
- Communicating to IOO's in this domain must not rely on controlled access information. Almost all recipients are unable to access privileged information. Need to package alerts and warning per "plain language guides."[2]

[2] https://www.plainlanguage.gov/

- ISAO or ISAC needed in addition to using NCCIC or CISA as the primary platform for information sharing for traffic agency systems.
- Better understanding of how information flows between the FBI, DHS Cyber, and State and Local LE required.

The following findings pertain to the communication protocol between IOOs/transportation stakeholders and security researchers:

- Independent security researchers do not see an incentive to share discovered vulnerabilities with users in this industry.
- Security researchers do not have any way to determine to whom it is safe to report vulnerability discoveries.
- Frequently vulnerabilities are not reported, as the penetration testing community sees no benefit in sharing information with transportation system equipment manufacturers, owners, and operators. They are frequently viewed as criminals and do not know who to report to that will take them seriously. Security researchers would like to get credit for a vulnerability discovery. This can be a problem whether reporting the vulnerability to an ISAC, equipment manufacturer or IOO, who in general do not want to publicize the vulnerability.
- Most attractive targets in this sector are high visibility devices and services (i.e., dynamic message signs, cameras, etc.). However, the targets that could cause the greatest safety issues are traffic controllers. So, the most likely target is not the same as the most damaging targets.
- This community is further discouraged from reporting vulnerabilities since they need feedback to show their reports are being acted on. This often happens in the timeframe substantially shorter than the norm in the transportation sector.
- Security Researchers may pay more attention to traffic systems, helping the transportation field improve awareness of vulnerabilities if given the opportunity for financial reward. A bug bounty program is also a good mechanism to encourage vulnerability sharing.
- Other security researchers could be encouraged to share vulnerabilities if they were able to report anonymously to a reporting mechanism.
- Municipal agencies and IOO’s typically do not have established procedures to handle unsolicited reports from security researchers. Many do not have defined cyber security reporting structures.
- Public municipal agencies and IOO’s generally do not monitor active cyber vulnerability reports unless it is part of local law enforcement objectives or they have dedicated cyber security organizations (i.e., New York, Washington DC, Los Angeles, etc.). Some agencies are members of existing ISACs such as Multi-State ISAC (MS-ISAC). Smaller agencies typically rely on information flowing from better-funded agencies that can afford the annual ISAC membership fees.

The following findings pertain to the communication protocol between IOOs/transportation stakeholders and ISACs:

- ISAC/ISAO/NCCIC will need access to domain-specific SMEs to help analyze vulnerability reports. Interpreting, validating, and developing mitigations from reported vulnerabilities will require assistance from equipment manufacturers and vendors. They will also need input from IOO’s to quantify or estimate impact to the public in terms of safety and mobility risks. This group generally has a better process to handle unsolicited vulnerability reports. The amount of information needed is seen as a barrier to some independent security researchers, as discovery of a vulnerability is often made during activities with uncertain legality. If a crime was committed during the vulnerability discovery process, law enforcement agencies must act on the crime which further discourages vulnerabilities from being shared.

Lack of Communication when Responding to Cyber Incidents

The following findings were captured from Stakeholders regarding cyber incident response:

- Most agencies do not have a cyber-incident response plan indicating who manages the incident and who to report to within the agency and externally (i.e., law enforcement). Where plans exist, System operators may never see the plans and it is doubtful both Informational Technologies (IT) and Operational Technologies (OT) have validated those plans together. Those that show capabilities beyond this probably have never exercised the plans they possess.
- Cybersecurity incidents are still fairly rare, so many organizations do not have much experience dealing with them.
- Law enforcement is frequently first to be called in response to an active cyber incident. However, they are not SMEs and will need assistance to identify the cyber incident's nature and severity of impact, using a common criterion. Additionally, they will need to know how they can collect forensic evidence, especially with regards to mission-critical equipment that may be affected.
- Major incidents are frequently handled via local law enforcement and do not necessarily communicate these incidents to national reporting systems. This increases the time it takes to identify national level or rapidly spreading incidents. As noted above, not all stakeholders have an incident response plan, and those that do, frequently have never reviewed, or practiced it. National information sharing organizations do not have easy access to equipment manufacturer representatives or transportation SMEs in responding to incidents.

Existing Funding Rules, Voluntary Contracting and Procurement Language Needed for Organizational Changes

The following findings were captured from Stakeholders regarding the use of existing funding rules for potential organizational changes:

- There can be a role for contracting and procurement to alter the current state of practice.
- Equipment Manufacturers and vendors will need customer demand (currently absent from almost all interactions) to increase cyber resilience of manufactured devices. Equipment manufacturers are ready to offer solutions, but they cannot support it if their customer refuses to pay for the additional resilience. The market frequently operates on a low bid environment, and they are unable to compete by offering features customers view as extraneous.
- Role of contactors and system integrators are frequently ambiguous. This acts as a layer of insulation for security and resilience information to flow between agency operators and equipment manufacturers.

Chapter 3. Current Landscape

There are a variety of cybersecurity incident organizations that provide some mechanisms for information sharing. Within the transportation landscape, there currently exists four transportation-focused information sharing organization types: Fusion Centers, ISACs, CISA, and Emergency Operation Centers.

To understand how the existing information sharing organizations collaborated in transportation cybersecurity information sharing, the research set includes the following:

- Determine the current way ISAOs are used for information sharing and if there are any gaps in existing guidance that do not address transportation infrastructure requirements.
- Identify necessary ISAOs.

Before evaluating available ISACs, the criteria utilized to conduct initial selections includes an examination of the following:

- Support of transportation infrastructure cybersecurity reporting and information exchange.
- Consideration of existing ISAC characteristics.
- Communication channels with other information sharing organizations.
- Knowledge sharing regarding transportation infrastructure cybersecurity features, requirements, and gaps in existing guidance for sharing cyber incident information.

Previous findings from the 2017 USDOT FHWA project were utilized to assist in gap understanding, along with pertinent cybersecurity information sharing and incident management guidance and recommendations from the DHS, National Institute of Standards and Technology (NIST), and others on cybersecurity information sharing and incident management of other relevant programs such as the National Cooperative Highway Research Program (NCHRP) (03-127) on “Cybersecurity of Traffic Management Systems.”

After evaluating existing ISAOs for their transportation relevance, the following information sharing organizations best suited for transportation were identified:

- ISACs—Various ISACs across industries that discuss topics relevant to transportation cybersecurity.
  - Auto-ISAC—Will often gather information received in Transportation ISAC reports and disseminate this information to their members through email. To submit a report, the Auto-ISAC maintains a web form available to the public through their website, and, if a report is submitted by a member, analysts working with the Auto-ISAC will consult a database of vulnerabilities to establish trends, do research, and conduct investigations.
  - MS-ISAC—Provides cybersecurity information sharing through email/reports to multiple state organizations with the intent of improving the Nation’s cybersecurity posture. The MS-ISAC deploys and manages intrusion detection sensors called Albert, which are deployed in all 50 states. Their incident response team monitors detected intrusions around the clock every day.

Based on these intrusions, a threat map is maintained and available to members as well as a monthly report. To submit a vulnerability, the MS-ISAC provides a hotline, an email, and a web form available to the public. Upon receiving a vulnerability, the MS-ISAC maintains an emergency response team to assist with any cyber events.

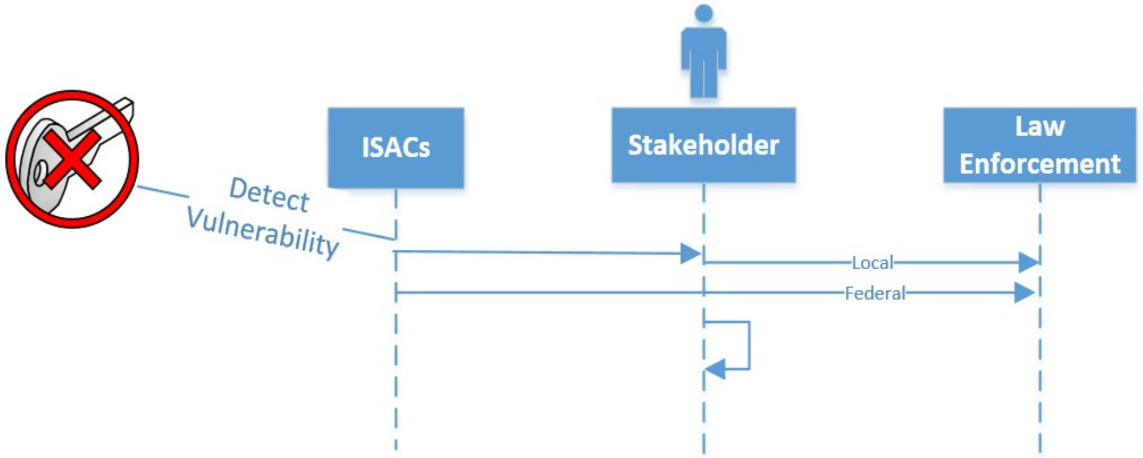
    - ST-ISAC (Surface Transportation Information Sharing Analysis Center) and PT-ISAC (Public Transportation Information Sharing and Analysis Center)—Where domain-specific security information sharing regarding freight and passenger railroad and non-railroad surface transportation sector is needed, the ST-ISAC and their collaborative ISAC, the PT-ISAC, are available. The ST-ISAC is sponsored by the Association of American Railroads (AAR) and the PT-ISAC Sponsored by the American Public Transportation Association (APTA). These ISACs provide cybersecurity and physical security information to members and partners via email reporting. The ISACs maintain a hotline and email services through their shared website. Research team efforts to gather process information through phone calls and email requests for information, found the site services were only responsive to membership requests.

- CISA—Supports vulnerability reporting and information sharing. It is recommended that IOOs report to CISA through their web portal which will provide the correct format for submitting a report as well as ensure that an emergency response representative will get in contact with the submitter.
    - NCCIC—Under DHS/CISA and serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts.
- Fusion Centers—Fusion Centers look to provide front-line law enforcement, emergency services, public safety, and private sector security personnel with resources to gather and share threat-related information. They are categorized into two types: Primary, which represent the entire state, and Recognized, which represents a region or major urban area within a state. Fusion Centers have three main functions: performing cyber/physical security assessments of their area of responsibility, monitoring/analyzing events or follow up with anonymous tips, and presenting and educating on cyber events/topics. Fusion Centers are often collocated with Federal and local law enforcement, providing a direct path for cyber incident sharing.
    - Our team conducted interviews with various Primary and Recognized Fusion Centers resulting in the specific characteristics below as identified by the Fusion Centers:
        - Fusion Center #1.
            - Partnered with DHS to train cyber staff.
            - Maintains a distribution list to members.
            - Distribute cyber-threat bulletin to public, compiled and translated by analysts working in Fusion Center.
            - Send alerts based on open source (discovered by analysts) or partner information.
            - Part of the Cyber Intelligence Network, a multi-agency community, that connects the cyber portions of fusion centers and other agencies through a collaborative platform hosted on the Homeland Security Information Network (HSIN).
            - Collaborates with neighboring states for regional, state, and local cyber threats.
            - Actively monitors dark websites (websites with restricted access that are meant for disseminating information to black-hat hackers).
        - Fusion Center #2.
            - Retain a Threat Liaison Officer (TLO) onsite.
            - Maintains a watch center at their fusion center to monitor active threats.

    - Receives enquiries from Law Enforcement for monitoring and analysis.
    - Maintain a mailing list that includes transportation members.
  - Fusion Center #3.
    - Maintains an anonymous tip reporting system.
    - Present to and educate both public and private sectors on cyber related topics.
    - Fast tracks incidents to mitigate and handle the incident.
    - In contact with DHS, CISA, FBI, MS-ISAC, and Elections-ISAC.
  - Fusion Center #4.
    - Civilian workforce, funded through state DHS.
    - No investigative power, which hinders their organization in terms of access.
    - Maintain analytic portfolios on domestic/international terrorism, organized crime, school safety, cyber security, critical infrastructure, and social media.
    - Maintain an anonymous tip line through schools.
    - Disseminate information through TLO program.
    - If they receive information pertinent to private sector, share with private sector as well.
    - Non-urgent Incidents they put on HSIN.
    - If an incident is urgent, they will directly contact ILO.
    - Office is collocated with Transportation ILOs.
    - Suspicious activity—prefer to reach out to them and then they reach out to Federal, state, and local law enforcement.
    - Maintain a one-way relationship with LE.
    - Analyst is on call after hours for urgent events.
- Emergency Operation Centers (EOCs)—These centers implement plans and programs to help prevent or lessen the impact of emergencies and disasters. Some centers will implement programs to increase public awareness about threats and hazards, coordinate emergency planning, provide an array of specialized training for emergency responders and local officials, and administer disaster recovery and hazard mitigation programs. EOCs typically are not cyber experts and will need to consult with external organizations to plan response and recovery from the impacts of cyber vulnerabilities.

Figure 1-4 depict the existing information flow between information sharing and analysis organizations and stakeholders. Each of the ISACs indicated their communication flows from their own perspective as captured the diagrams.

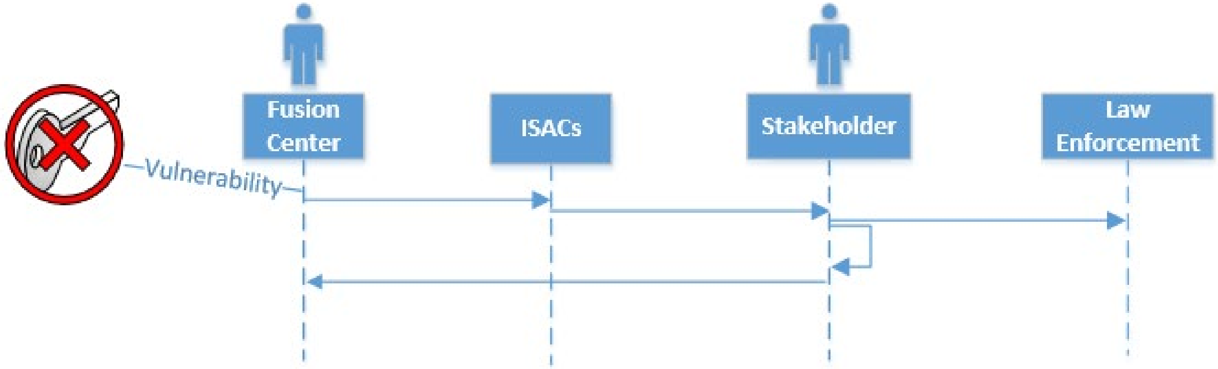
As shown in Figure 1, this diagram indicates the current flow of cyber incident information exchange when a vulnerability is detected by an ISAC. The ISAC will first disseminate information to its members, who may then share to other stakeholders and to their local law enforcement who may not be aware of the vulnerability (not guaranteed). The ISAC will also share information with Federal law enforcement, who may then continue sharing (not guaranteed).



Source: FHWA

Figure 1. Flowchart. Current flow of cyber incident information exchange when an Information Sharing and Analysis Center detects vulnerability.

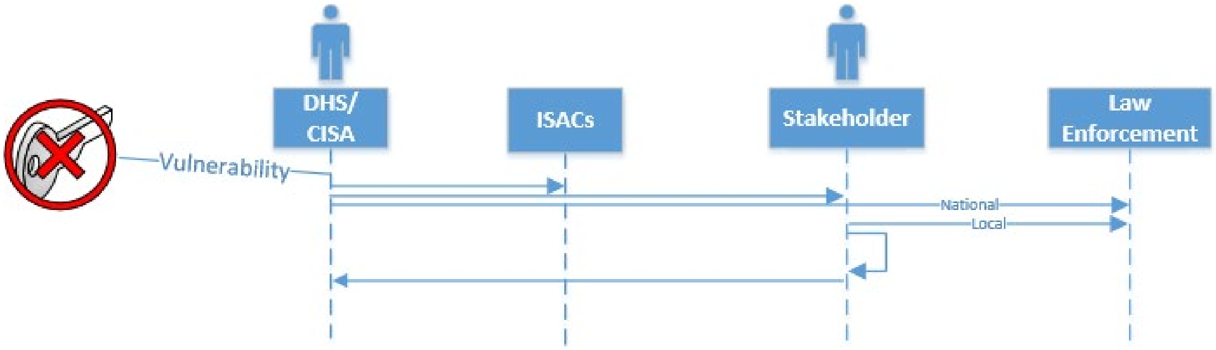
As shown in Figure 2, this diagram indicates the current flow of cyber incident information exchange when a vulnerability is detected by a Fusion Center. The Fusion Center will first disseminate information to its known ISACs, such as the MS-ISAC, who then shares this information with their members (stakeholders). Stakeholders may then communicate cyber incident information to other stakeholders and to their local law enforcement who may not be aware of the vulnerability (not guaranteed). Stakeholders will then work with the Fusion Center to resolve any vulnerabilities.



Source: FHWA

Figure 2. Flowchart. Current flow of cyber incident information exchange when a fusion center detects vulnerability.

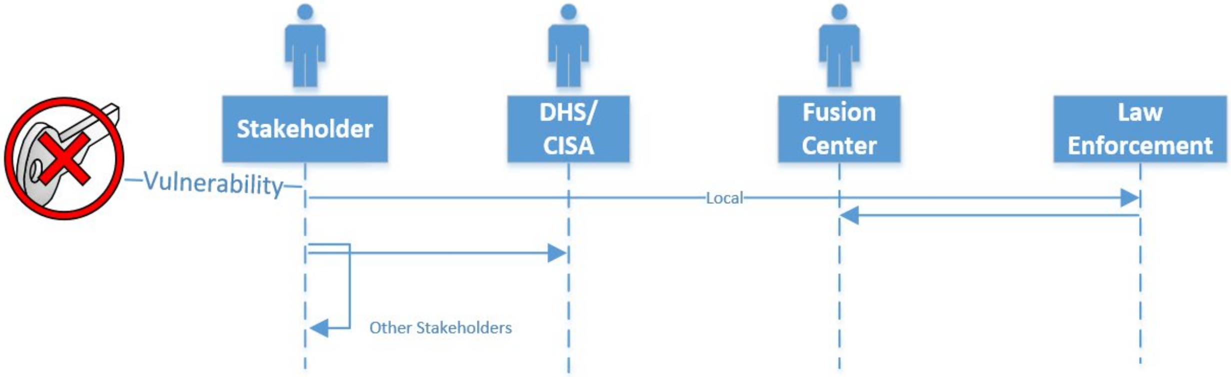
As shown in Figure 3, this diagram indicates the current flow of cyber incident information exchange when a vulnerability is detected by DHS/CISA. DHS/CISA will disseminate information to three groups in parallel: ISACs (such as the MS-ISAC), stakeholders, and national or Federal law enforcement. Stakeholders may then communicate cyber incident information to other stakeholders and to their local law enforcement who may not be aware of the vulnerability (not guaranteed). Stakeholders will then work with DHS/CISA to resolve any vulnerabilities.



Source: FHWA

Figure 3. Flowchart. Current flow of cyber incident information exchange when the Department of Homeland Security/Cybersecurity and Infrastructure Security Agency detects vulnerability.

As shown in Figure 4, this diagram indicates the current flow of cyber incident information exchange when a vulnerability is detected by a stakeholder. Stakeholders will first disseminate information to their local law enforcement, who will then share cyber incident information to their associated fusion center. Stakeholders may then communicate cyber incident information to other stakeholders and to their national/Federal law enforcement agencies, such as DHS/CISA, who may not be aware of the vulnerability (not guaranteed).



Source: FHWA

Figure 4: Flowchart. Current flow of cyber incident information exchange when a stakeholder detects vulnerability.

These identified organizations represent the current transportation cybersecurity communication network available to stakeholders. Based on these identified capabilities, and the problems identified previously, recommendations and process improvements will be created to improve the communication protocols and procedures used by stakeholders.

Chapter 4. Minimum Requirements for Solution

In consideration of cyber incident reporting and information exchange, there are several transportation cybersecurity features or aspects to consider. Transportation infrastructure systems come in a variety of equipment configurations based on the agency deployment size, needs, and resources. As determined by SwRI in the Transportation Research Board (TRB)/National Cooperative Highway Research Program (NCHRP) project 03-127 titled "Cybersecurity of Traffic Management Systems," currently planned to be released at https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179, the equipment used in these systems fall within one of four categories:

- Safety Critical—systems used to maintain safe driving conditions.
- Active Systems—systems used to actively change traffic conditions.
- Networking Equipment—systems that transmit and route information to other systems.
  - May be classified as either field or center equipment, depending on the location.
- Passive Systems—systems that provide information to users (aka drivers) or other traffic systems.
  - May consist of data transfer (i.e., weather, road conditions) or messages to users.
- Operation Critical—systems used in a transportation infrastructure system to manually adjust traffic conditions as needed.

Each these systems consist of different levels of safety criticality and may contain sensitive information. Note that attacks on a device in one of the categories may affect the operations of a device in another category. For example, an attack on networking equipment (i.e., firewall hardware, routers, switches) could affect the communications of active systems (i.e., traffic controller) and increase the safety criticality of such an attack. Using these equipment categories, we are able to address operational impacts that may span an entire transportation system.

Additionally, there may be the desire to withhold pieces of sensitive information for the purpose of criminal investigation. As such, the following are some transportation cybersecurity aspects that infrastructure systems should involve:

- Protection of sensitive and personally identifiable information (PII).
- Ensuring CIA (Confidentiality, Integrity, and Availability) of stakeholders.
- Implementation and usage of useful analytics.
- Continuous monitoring of networks for anomalies.
- Compliance with security standards/best practices.
- Threat prevention and patch management.

Using these different aspects will not only increase the cyber resilience of the transportation infrastructure systems in place, but they will also assist in the response and reporting of cyber incidents.

Based on these considerations and the current landscape identified, the following data requirements were determined to provide the minimum information needed to assist stakeholders in cyber incident information exchange:

- Common Vulnerability Metrics.
  - Suggest Common Vulnerability Scoring System (CVSS) (https://www.first.org/cvss/).
  - To best share information about the risks associated with vulnerabilities, these risks should be quantified. These allow stakeholders of all backgrounds to understand severity of vulnerabilities by using a common language.
  - Included in "Data Exchange Specifications Applicable to Incident Handling" table in NIST 800-61 rev. 2.
- Traffic Light Protocol—https://www.us-cert.gov/tlp.
  - A set of designations used to ensure that sensitive information is shared with the appropriate audience. This is used as a quick and easy identifier to ensure that the proper information is reaching the proper stakeholders.
  - Not mentioned in NIST 800-61 rev. 2, but discussion of taking care who receives certain information "Otherwise, sensitive information regarding incidents may be provided to unauthorized parties, potentially leading to additional disruption and financial loss."
- Equipment Vendor Effected.
  - This will detail what equipment manufacturer or vendor is affected and ensure that this equipment manufacturer receives proper support.
  - Discussion of sharing with "affected external parties" and software vendors included in NIST 800-61 rev. 2.
- Equipment Models Effected.
  - This will detail what hardware and/or software system is affected so that other stakeholders with the same device might make changes to the device to avoid the identified vulnerability.
  - Discussion of sharing with "affected external parties" and software vendors included in NIST 800-61 rev. 2.
- Vulnerability overview (i.e., Critical Infrastructures effected, Areas deployed).
  - An overview of the vulnerability will provide stakeholders both educational and security information regarding a vulnerability. These are both necessary in the prevention of and recovery from vulnerabilities that match or are similar to the current vulnerability.
  - Discussion of dissemination of vulnerability information in "Advisory Distribution" section of NIST 800-61 rev. 2.
- Mitigation Recommendations, if available.
  - If a mitigating recommendation has been found, it will explain to stakeholders what is necessary to reduce the risk of the vulnerability. Typically, this will involve specific actions to take on the stakeholder's end.

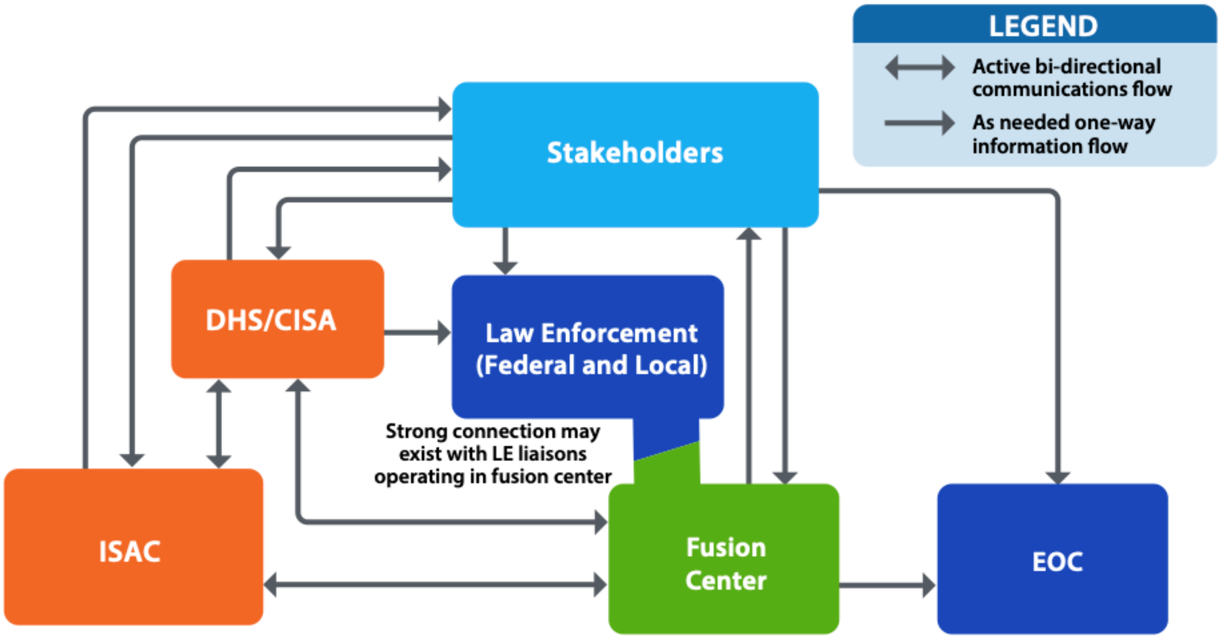
- Discussion of follow-up reports/lessons learned meetings throughout NIST 800-61 rev. 2. These reports/meetings should discuss mitigation strategies and preventative measures.

This information should be shared as part of a vulnerability report upon vulnerability discovery by an IOO, Chief Information Security Officer (CISO), or other affected organization. In consideration of the minimum requirements, two other constants were identified to ensure effective information sharing:

- Each municipal and/or state IOO should maintain a working relationship with their own or their state CISO or Chief Information Officer (CIO), such that in the case of a cyber incident, these personnel will be readily available to assist.
- IOOs should also maintain contact with their Fusion Center either directly or via their respective CIO/CISO.

As cyber incidents are investigated, transportation stakeholders are realizing that agency response activities and liability responsibilities to cyber threats are very similar to physical safety threats (i.e., fires, thefts, etc.). As such, they are processing these incidents in similar fashions since incidents must be reported to law enforcement for insurance purposes. To assist state agencies and other transportation stakeholders, Fusion Centers provide an all-in-one location to report localized cyber and/or safety incident. Additionally, Fusion Centers provide cyber incident sharing through their direct lines to DHS CISA and the MS-ISAC.

This provides the simplest path for transportation infrastructure stakeholders to report incidents, as each state contains a Primary Fusion Center providing statewide analysis. Some states may designate additional Fusion centers, called Recognized Fusion Centers, that serve a major urban area. When available, stakeholders can automatically subscribe to cyber incident information if they set up a monitoring system to DHS CISA's AIS service. Information sharing and analysis organization memberships, primarily the MS-ISAC and DHS CISA's AIS, can then best be utilized by stakeholders as a resource for cybersecurity education and cyber incident information exchanges concerning topics effecting the transportation industry. Government organizations, such as FHWA and USDOT, can also leverage these ISAOs to share information, similar to how DHS or LE would. Given the resources that can be provided by the different levels of information sharing and analysis organizations, Figure 5 shows the recommended cyber incident information exchange path. A bi-directional communication flow indicates that points of contact in each agency are in direct communication with each other, while a one-way information flow indicates that information is pre-formatted and provided on an as-needed or as-available basis. In this diagram, the strong connection between "Law Enforcement (Federal and Local)" and "Fusion Center" is modeled to show that in most cases, there are one or more law enforcement representatives working closely with or supporting the operations of the fusion center. Additional details such as the data that is provided are expanded in later research efforts. Note that this information path does not provide any indication of timing, as none of the ISAOs researched in this effort provided information regarding response times.


LEGEND
Active bi-directional communications flow
As needed one-way information flow
Stakeholders
DHS/CISA
Law Enforcement (Federal and Local)
Strong connection may exist with LE liaisons operating in fusion center
ISAC
Fusion Center
EOC

Source: FHWA

Figure 5. Flowchart. Recommended flow of cyber incident information exchange.

Chapter 5. Proposed Improvements

The following sections detail the necessary steps to create an improved transportation stakeholder cybersecurity communication framework.

Recommendations Based on Findings Regarding the Current State of Information Sharing

This section details recommendations for each of the problem areas identified in the “Problem and Need” section of this document.

Culture Changes for Transportation System Cyber Resilience

Based on the findings from “Problem and Need” regarding the current culture surrounding transportation system cyber resilience, some of these needed changes could be facilitated by leveraging the requirements for funding that comes with USDOT. Such changes should be worked out in detail with USDOT management to move forward. Examples of changes can include:

- Cyber resilience as an element for system resilience when evaluating Federal aid eligibility. For example, the citations from the order page for FHWA Order 5520 (https://www.fhwa.dot.gov/legsregs/directives/orders/5520.cfm) represent a good model to start from in creating similar citations for cyber resilience.
- Consider investigating possible provisions that could be incorporated into architecture and best practices for Intelligent Transportation Systems (ITS) projects that would address cyber resilience issues.
- Consider how patch updates to field devices can be made part of the cyber resilience requirement.
- Create suggested procurement languages for ITS equipment that includes improved resilience.
- Study/investigate cyber resilience consideration in 940.11 rule[3] or defining application that would establish transportation organization to consider cyber security.

[3] https://www.fhwa.dot.gov/legsregs/directives/fapg/cfr0940.htm

Process to Promote Information Sharing Regarding Cyber Risks/Vulnerabilities Between Infrastructure Owner Operators, Equipment Manufacturers, Law Enforcement, and Independent Security Researchers.

Based on the findings on the current problems facing information sharing between transportation stakeholders in “Problem and Need,” the following recommendations were generated:

- An anonymous tip/information mechanism is needed as an option for security researchers to share cybersecurity vulnerability information.
- Operators, equipment manufacturers, and equipment manufacturer representatives need to establish feedback mechanisms for security researchers.
- We need to identify a common criterion (hopefully adopting an existing one) to describe severity and criticality of cybersecurity information.
- There needs to be clear communication channels for cyber security information flow between IOO, equipment manufacturer that supply IOOs, Government, and security researchers.
- Insert a protection clause into the procurement contract to protect security researchers when sharing vulnerability information with equipment manufacturers.
- A bug bounty program will encourage security researchers to research vulnerabilities in this sector. Perhaps a “challenge coin” system, where security researchers can receive recognition for their security discoveries, could be used along with a traditional bug bounty program.
- Promote the use of the bug bounty program to encourage exploration into vulnerabilities of transportation systems.
- IOO’s should have multiple avenues to report issues but need directions in cases short of actual incidents or attacks.
- Establish a regular communication channel between national organizations and operators. Ideally this should be a channel that already exists and is available 24/7/365.
- There should be simple contacts from this group to help national information sharing organizations assess the risk to safety and operation from a cyber-vulnerability.

Defining Communication Procedures and Best Practices when Responding to Cyber Incidents

Based on the findings on the current problems facing communication during incident response in “Problem and Need,” the following recommendations were generated:

- Transportation Operators need to develop cyber-incident response plans specific to their agency.
- Transportation Operators need to follow consistent practices when reporting cyber security incidents to help detect the spread and severity of fast-moving cyber storms.
- There should be a simple SME contact for cyber security response available to all stakeholders for obtaining the necessary level of support.

Clarifying Existing Funding Rules, Voluntary Contracting and Procurement Language for Organizational Changes

Based on the findings on the current problems facing existing funding rules, voluntary contracting, and procurement language in “Problem and Need,” the following recommendations were generated:

- Encourage consideration of cyber resilience designs in field equipment by offering sample contracting languages that can be used in IOO purchasing contracts.
- Clarify the role of contractors and system integrators when a cyber incident occurs.
- Changes in roles and responsibilities to contractors and systems integrators may need to be addressed in contracting documents. This can include some languages to incentivize equipment manufacturers to correct discovered vulnerabilities or participate in some form of bug bounty program.
- Contracting documents could address the equipment manufacturer’s relationship with security researchers.
- Suggest we develop procurement languages with a protection clause for bug reporting by independent security researchers. This will help to create trust between the security researchers in the penetration testing community and equipment manufacturers.
- Establish rules to encourage and protect security researchers that share vulnerability information.
- Clarify the connection between system resiliency consideration as part of system engineering analysis to meeting 940.11 rule.
- Develop/standardize the reporting criterion for a cybersecurity incident.
- Investigate the adaptation of FHWA Order 5520 in creating cyber resilience directives. Also consider the work the New Jersey Division Office has started with New Jersey Department of Transportation.

Develop Strategies to Establish Consistent Usage of Cybersecurity Terminology

Given the different responsible parties within stakeholder organizations that need to communicate to operate a resilient transportation system and provide some level of response during a cybersecurity incident, a common language that provides a common understanding of the language’s usage was needed. To develop a common understanding between stakeholder organizations, various terminologies were consolidated that can help the transportation and cybersecurity community and improve understanding and conversations related to transportation cyber incident information sharing. Relevant terms were identified through collaboration with NCHRP, the Transportation System Cyber-Security Framework (TSCF) partners, and other stakeholders.

The resulting glossary is shown in Appendix C of this document.

Develop/Adapt Cybersecurity Incident Communication Protocols

Previous research examined existing ISACs and other ISAOs and how they could best support transportation infrastructure and cybersecurity information exchange. The following are the roles and responsibilities of existing organizations, along with stakeholders and other agencies involved to be considered for cybersecurity incident communication protocols:

- Municipal IOO.
  - **Role:** The main role of the municipal IOO is to ensure that all traffic operations within a TMC are maintained during an incident. Because they do not have the resources of a state IOO, their role involves escalating the incident to the state IOO level to ensure that the proper resources are brought to the table. Their participation in the reporting process will be largely dependent on their own cyber maturity and the presence of officials such as a municipal CISO.
  - **Responsibilities:** Once a cybersecurity incident has been identified, a municipal IOO is responsible for executing their cybersecurity incident management plan (IMP), if available, or similar security procedures and ensuring they are followed through to response completion. This process may include contacting OT staff, IT staff, and/or subcontractors that are involved in system integration and safety and maintenance operations for the effected systems to confirm the incident and determine the vulnerability's risk. Additionally, if the IOO has a municipal CISO, the cybersecurity incident is reported to the municipal CISO to aid in coordinating the vulnerability information exchange process. If the IOO does not have a CISO, then the state CISO is to be alerted so that they can coordinate vulnerability information exchange with law enforcement, nearby Fusion Centers, MS-ISAC, and other IOOs. The information exchange with appropriate parties follows the cybersecurity IMP's direction and include vulnerability information with at least the minimal details as described in the Vulnerability Report Template provided in Appendix B.
- State IOO.
  - **Role:** State IOO's role is to ensure that traffic operations are maintained within their TMC, therefore, they are involved with the immediate response and mitigation of both ongoing attacks and discovered vulnerabilities. They also serve as a key source of information regarding the exact details of the attack. Reporting those details accurately and rapidly is a key part of ensuring that the proper parties are brought in, both to combat the initial vulnerability and ensure that other parties are alerted and can protect against it.
  - **Responsibilities:** Over the course of an incident, the state IOO is responsible for implementing their cybersecurity IMP, if available, or similar security procedures to address the incident in progress. Included within that plan are instructions for workers performing safety-critical and maintenance operations. Vulnerability information is exchanged during cybersecurity incident reporting to the State CISO/CIO, with at least the minimal details as described in the Vulnerability Report Template to determine the appropriate parties for further disclosure. CISO/CIO will then be responsible for distribution of the vulnerability information to the appropriate parties.
- Equipment Manufacturer.
  - **Role:** In many cases, equipment manufacturers will be the first to discover a vulnerability whether through internal testing or through an active cyberattack. In those cases, its primary role is to share information to the correct parties and instigate mitigation measures to protect against the attack or vulnerability.

  - **Responsibilities:** The first responsibility of an equipment manufacturer in the event of a cybersecurity incident is to implement their incident response plan. Following that, they are responsible for sharing that information with the relevant groups. The first contact is with the affected IOOs. Depending on whether the vulnerability is being actively exploited or not; that contact may be required within 24-48 hours. A Vulnerability Report is provided as part of the disclosure process. Following contact with the IOOs, the equipment manufacturer also shares the vulnerability information with the relevant ISACs.

- Security Researcher / SME.
  - **Role:** Security researcher's or SME's role in the cyber incident process is typically the discovery and disclosure reporting of security vulnerabilities to the system's owner operator, a vulnerability 3rd party anonymizer, or the equipment manufacturer. After vulnerability disclosure, security SMEs may also be called upon to serve as experts on the details of the vulnerabilities.
  - **Responsibilities:** There are several different ways that security researchers can disclose vulnerabilities that they discover. The primary manners considered within this project are disclosing them directly to the equipment manufacturer, disclosing them to a third-party anonymizing organization, or disclosing it publicly. If the researcher chooses to disclose the vulnerability directly to the equipment manufacturer, the first step is organizing the key vulnerability in a manner such as a Vulnerability Report Template. This information is then provided to the equipment manufacturer. In addition, the information is provided to the relevant IOOs, whether municipal or state. The other two manners of disclosure place the responsibility for distribution of vulnerability information on other parties, such as the third-party organization or groups such as Federal law enforcement that look for publicized vulnerabilities.
- Law Enforcement.
  - **Role:** The role of law enforcement in incident response centers around investigation may include attribution after the incident occurs or may involve discovery of vulnerabilities through other investigations or monitoring of public sources.
  - **Responsibilities:** In cases where law enforcement is the first to discover a vulnerability, the first responsibility of law enforcement is to disclose it to the affected IOO. This allows them to manage the reporting process. When reporting to law enforcement, reports are first made to local law enforcement, as they have the responsibility of escalating the report, as necessary. As fusions centers are often collocated with individuals in law enforcement, law enforcement will share information with fusion centers to ensure it reaches the larger group of transportation stakeholders. Information sharing groups such as ISACs may also aid in reporting vulnerabilities to law enforcement.
- Fusion Center.
  - **Role:** The key role of fusion centers during an incident is information sharing. Through their cybersecurity evaluation processes and education roles, they are connected with many of the key players in the areas that they are based in. Their roles are typically tailored based on the needs of the area that they are based in; however, they may also serve a role in reporting vulnerabilities that are discovered through their research and reporting capabilities.
  - **Responsibilities:** Fusion centers typically have significant involvement in law enforcement and the Federal Government. They are responsible for ensuring that the right contacts within Government and law enforcement receive the vulnerability report.
- MS-ISAC.
  - **Role:** The key role of an MS-ISAC is to provide vulnerability information to their members by facilitating communication between IOOs. The vulnerabilities that they report can come from IOOs

or be detected by the MS-ISAC. They can also provide support to stakeholders who discover vulnerabilities within their systems by offering expertise and support.

- **Responsibilities:** During a cyber incident, the MS-ISAC may be reached out to for reporting purposes as well as support. The first responsibility of the MS-ISAC is analysis to determine whether the cybersecurity incident represents an emergency situation. If it does, an update is sent out to members as soon as possible to members with instructions on how to address the vulnerability. In cases where the MS-ISAC discovered the vulnerability, an immediate update is sent to all relevant stakeholders to allow them to address the vulnerability. During the period of cybersecurity incident response, the MS-ISAC also works with the stakeholders to establish their proper response. This can include offering MS-ISAC resources such as emergency conference calls, forensic or log analysis, mitigation recommendations, and reverse engineering. In the time period following the initial cyber incident, the vulnerability will also be reported in the anonymized monthly summary of cyber incidents during that timeframe.

With focus on transportation industry-specific resources, two transportation-focused ISACs exist: MS-ISAC and the Surface Transportation Information Sharing Analysis Center (ST-ISAC). These ISACs provides resources for cybersecurity education and cyber incident information exchanges however concerns exist regarding ISAC membership cost and organizational limitations. One such concern is that the MS-ISAC only allows public state agencies to join; meaning that state contractors who may be performing the safety-critical roadway and maintenance operations are excluded (unless working with a public agency)—this is considered a major information exchange gap. Also, the ST-ISAC offers little specifics on its site regarding transportation-related cybersecurity information they share with their members (e.g., focused on railroad-relevant vs. traffic). Further, information available regarding the ST-ISAC is related to rail or surface transportation-related topics, which may be of less value to the specifics that stakeholders in a DOT would look to gain information on if they were members. As the MS-ISAC provides and receives cybersecurity-relevant information from each of the states, they are to be considered a larger, central resource of cybersecurity relevant information.

Additionally, Fusion Centers, consisting of statewide Primary Fusion Centers and localized, major urban Recognized Fusion Centers, provide stakeholders (including the public) a central location to report localized cyber and safety incidents and coordinate with Federal and local LE. Fusion Centers participate in cyber incident sharing by setting up relationships and having direct lines to organizations like DHS/CISA and the MS-ISAC.

Fusion Centers assist stakeholders by providing a simple path for reporting and seeking assistance in getting assistance with cyber incidents. However, Fusion Centers do not have the same capabilities and resources as information sharing organizations. Membership to ISAOs (such as MS-ISAC) will be IOOs' best option for access to topics affecting the transportation industry nationwide along with adjacent technologies affecting transportation infrastructure.

Through identification of improvements shown above, the research team was able to identify six (6) representative use cases, with both active and non-active attack scenarios shown in Appendix A, that illustrate the communication flow and decisions that need to be made for effective cyber incident information exchange. These six (6) use cases provide assumptions and outline procedures to follow prior to and during an active cyber-attack. A summary of the use cases and their process flows is as follows:

- **Use Case 1—Municipal IOO—**Provides a process to follow when either an active or non-active cybersecurity incident is discovered. Example usage by a municipal IOO is shown below for both cases.

  - *Municipal IOO discovers a vulnerability running on their devices that has not been used in an attack (to their knowledge).* We recommend using the process in UC1-S1 (Page 35), which has them confirm the vulnerability, execute their IMP, and inform the equipment manufacturer, system integrators/internal contractors, and municipal/state CISOs where applicable.
  - *Municipal IOO discovers a vulnerability running on their devices that is actively being used in an attack.* We recommend using the process in UC1-S2 (Page 40), which has them confirm the vulnerability, execute their IMP, inform the equipment manufacturer, system integrators/internal contractors, and municipal/state CISOs, where applicable, and then includes either municipal CISO or direct (in the case of no municipal CISO) outreach to law enforcement.
- **Use Case 2—State IOO—**Provides a process to follow when either an active or non-active cybersecurity incident is discovered. Example usage by a state IOO is shown below for both cases.
  - *State IOO discovers a vulnerability running on their devices that has not been used in an attack (to their knowledge).* We recommend using the process in UC2-S1 (Page 48), which has them confirm the vulnerability, execute their IMP, and inform the equipment manufacturer, system integrators/internal contractors, state CISOs, and law enforcement (optionally), where applicable.
  - *State IOO discovers a vulnerability running on their devices that is actively being used in an attack.* We recommend using the process in UC2-S2 (Page 54), which has them confirm the vulnerability, execute their IMP, inform the equipment manufacturer, system integrators/internal contractors, and municipal/state CISOs, where applicable, and outreach to law enforcement.
- **Use Case 3—Law Enforcement—**Provides a process to follow when either an active or non-active cybersecurity incident is discovered. Example usage by a law enforcement is shown below for both cases.
  - *A vulnerability that is not part of an active attack is discovered by law enforcement.* We recommend using the process in UC3-S1 (Page 59), which has law enforcement first confirm the existence of the vulnerability then create a report using the minimum information needed to assist stakeholders in cyber incident information exchange, as previously discussed in this document. Following the creation of the vulnerability report, law enforcement informs the affected equipment manufacturer, gathers additional information for the vulnerability reports, establishes a responsible disclosure period, and identifies mitigation measures. In a parallel process, law enforcement shares the report and mitigation measures with the MS-ISAC and fusion centers to continue information exchange.
  - *A vulnerability that is part of an active attack is discovered by law enforcement.* We recommend using the process in UC3-S2 (Page 63), which has law enforcement create the vulnerability report as before, with mitigation measures included, but also immediately reaching out to fusions centers and the MS-ISAC to begin information exchange immediately.
- **Use Case 4—Security Researcher—**Provides a process to follow when a non-active cybersecurity incident is discovered. Example usage by a security researcher is shown below for both cases.
  - *A vulnerability that is not part of an active attack is discovered by a security researcher.* We recommend using the process in UC4-S1 (Page 67), which has the security researcher create a vulnerability disclosure following the contents previously identified in this document, and other procedures to inform the equipment manufacturer of the affected device and their state or municipality's CISO.
  - *A vulnerability that is not part of an active attack is discovered by a security researcher, but the security researcher fears they may face legal consequences from sharing information about this vulnerability.* We recommend using the process in UC4-S2 (Page 72), which has the security researcher work through an anonymizer organization to prevent any repercussions from discovering the vulnerability (i.e., network monitoring without consent). This organization acts as

the security researcher would, by sharing vulnerability information to law enforcement and other organizations.

- **Use Case 5—Equipment Manufacturer—**Provides a process to follow when information on a non-active cybersecurity incident is either discovered by the equipment manufacturer or received from a security researcher. Example usage by an equipment manufacturer is shown below for both cases.
    - *A vulnerability that is not part of an active attack is discovered by an equipment manufacturer.* We recommend using the process in UC5-S1(Page 76), which has the equipment manufacturer develop a patch for their systems, provide the patch to customers, then inform the MS-ISAC to begin information exchange.
    - *A vulnerability that is not part of an active attack is discovered by a security researcher and reported to an equipment manufacturer.* We recommend using the process in UC5-S2 (Page 80), which has the equipment manufacturer following the same procedures as before, but first working with the researcher to understand the vulnerability.
- **Use Case 6—Fusion Center—**Provides a process to follow when either information on an active or non-active cybersecurity incident is received. Example usage by a fusion center is shown below for both cases.
    - *A vulnerability that is not part of an active attack is reported to a fusion center.* We recommend using the process in UC6-S1 (Page 83), which has the fusion center receive a vulnerability report and identify mitigation measures. This report and mitigations are then shared in a parallel process with municipal/state CISOs, law enforcement, and the MS-ISAC. Note: Some fusion centers are operated by local police and have a direct line to law enforcement agencies.
    - *A vulnerability that is part of an active attack is reported to a fusion center.* We recommend using the process in UC6-S2 (Page 86), which has the fusion center execute the same actions above but modifies the mitigation measures to include actionable information for affected organizations. Also, the fusion centers coordinate with municipal/state CISOs, law enforcement, and ISACS, providing mitigation and incident response support until the attack is resolved.

Through the development of these procedures, two constants appeared to have significance to the process:

- Each municipal and/or state IOO should maintain a working relationship with their state CISO or CIO, such that in the case of a cyber incident, the state will be readily available to assist.
- IOOs should also maintain contact with their Primary and/or Recognized Fusion Center.

These relationships ensure that the IOO has contact with local/Federal LE and will also be able to receive some sort of mitigation and recovery assistance during a cyber incident. Additionally, Primary and Recognized Fusion Centers provide cyber incident sharing through their direct lines to DHS/CISA and MS-ISAC. This currently provides the simplest path for transportation infrastructure stakeholders to report cyber incident information, as each state contains a state-oriented Fusion Center.

On top of these, recommendations, procedures, and process improvements for each of the information sharing organizations were developed. Each of the improvements are listed by organizations as follows:

- State and Municipal IOOs.
    - **Clear lines of communication need to be established with their municipal CISO, State CISO, or Local Fusion Center before a cybersecurity incident.** These information sharing pathways establish a support structure for the IOO that allows them to focus on recovery and matters related to the restoration/recovery to operations. At the same time, these pathways also

allow the vulnerability information to be shared with other IOO who may be vulnerable to an exploit. To establish these communication pathways, it is recommended for state and municipal IOOs to establish a working relationship or an established line of communication with either their municipal CISO, state CISO, or local Fusion Centers.

- State and Municipal CISOs.
  - **State and Municipal CISOs need to be the liaisons between their IOOs and the cybersecurity community.** This includes filtering received cybersecurity reports and providing clear points of contact to IOOs. By filtering and assisting the IOO's information sharing process, the CISO is ensuring that reports are indeed something new and helping the IOO apply readily available mitigations, if available, while short circuiting the recommended process. The CISO can improve the information communication process through establishing clear channels of communication and taking the onus of dissemination of information off of the IOO that is directly addressing the vulnerability.
- MS-ISAC.
  - Per research and conversations with representatives from MS-ISAC regarding their current capabilities and an understanding of where their information sharing gaps exists, the following improvements have been identified.
    - **IOOs need to review MS-ISAC provided vulnerability notifications** to verify that the notifications are relevant to hardware and software in their environment. MS-ISAC provides vulnerability notification service to their members. Their notifications are a curated list of vulnerabilities taken from multiple other vulnerability notification services including *Bugtraq*.
    - **IOOs must have input into how curation and modification of vulnerability notification is accomplished,** who the Subject Matter Experts are making those determinations, and how they consider industry specific hardware and software in curation and modification decisions. MS-ISAC modifies any received vulnerability notifications before they are sent to members and use a template to explain the vulnerability and suggest mitigations or recommendations for additional protections for the affected assets. Per discussions with MS-ISAC representatives, these notifications will typically be released within 30 minutes to 12 hours after receipt by MS-ISAC.
    - **IOOs need to monitor for any MS-ISAC cybersecurity incident response services advertised to members,** as these services can act as a lifeline to many organizations in case of an emergency. MS-ISAC provides a Security Operations Center (SOC[4]) and CERT service to its members in responding to incidents. Those services are provided 24/7 and will work to coordinate with the stakeholder on the proper response to an incident and services can include: emergency conference calls, forensic or log analysis, mitigation recommendations, reverse engineering, as well as a verbal report 24 hours following the incident, and a written report one week following the close of the incident. Should an IOO or CISO need to report an incident, a contact phone number and email

[4] Security Operations Center—A combination of people, processes, and technology protecting the information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects. (https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf)

        address for use when a CISO is reporting a vulnerability can be found at https://www.cisecurity.org/isac/report-an-incident/.

        - **IOOs should monitor the MS-ISAC's monthly anonymized summaries for potential mitigation strategies to vulnerabilities identified,** as this information could allow IOOs (or CISOs) to prevent attacks to their systems. MS-ISAC provides a monthly anonymized summary of the incidents received from the community, shared at the Traffic Light Protocol (TLP) amber level, and will provide a short description of the incident as well as the recovery. This summary will also review lessons learned or present recommendations to benefit the larger community as a result. This monthly summary will be reviewed by IOOs and CISOs to understand the threats to the community at large and gain awareness of any incidents that may have systems similar to those that they have deployed.
        - **IOOs should attend the MS-ISAC's monthly call as there may be valuable information/training.** As a part of this call, there are many trends or recommendations presented that a member may not feel are applicable to their organization. MS-ISAC spends a portion of their monthly call reviewing trends or recommendations that have been made as a result of the incidents that they are responding to or receiving notification of through other information sharing channels. By adding information on mitigation or how attack trends may affect their members, the monthly call will be more effective in assisting their member's cybersecurity posture.
        - **IOOs and CISOs need to leverage MS-ISAC's Malicious Code Analysis Platform (MCAP) service** as part of their information sharing and analysis efforts to determine additional information regarding malware in case of an incident. MS-ISAC provides MCAP, which is described as a web-based service, to enable members to submit suspicious files for analysis in a non-public fashion. This service provides the analysis and information to allow for remediation when dealing with a distinct type of malware without the need to use a public service such as *Virus Total*.

- Fusion Centers.
    - **IOOs should maintain a working relationship or clear communication path with Fusion Centers,** as they also have unique monitoring capabilities. Reports similar to what is shared by the MS-ISAC should also be shared with IOOs to ensure that they are knowledgeable of potential vulnerabilities that could affect them. Fusion Centers receive threat information from the Federal Government and law enforcement, analyze that information in the context of their local environment, and disseminate that information to local agencies. Fusion Centers are uniquely situated to leverage their information resources, including the capability to actively monitor dark websites and gather details from active cyber incidents to facilitate the timely sharing of that information with their respective IOOs and CISOs. Also, reports that are delivered by anonymizer organizations need to be verified and investigated with regards to the extent and applicability of the vulnerability.
- Anonymizer Organizations.
    - **IOOs should work with reports received from anonymizer organizations just as they would if they had received a vulnerability report directly from a security researcher.** Anonymizer organizations work directly with security researchers and provide a protected communication conduit for information sharing that would otherwise not be available. Security researchers with good intentions may be hesitant to share their findings directly with the organization or equipment manufacturer due to concerns and ambiguities over legal issues.
- CISA.

  - **IOOs should monitor CISA published information (e.g., press releases, emailed information) for cybersecurity relevant information to the transportation sector.** Though CISA remains a useful resource for cybersecurity incident response measures, information regarding CISA's engagement in cyber incident communication is limited, as direct outreach to CISA resulted in little to no response.

Conduct Cybersecurity Incident Exercise

Following the definition of transportation's current landscape, minimum requirements for information sharing and recommendations for process improvements, the resulting proposed cybersecurity communication process needed to be compared against traditional processes. This comparison would quantify the actual process improvements regarding reach and speed of information dissemination during a cybersecurity incident event. To achieve this purpose, the research team prepared and conducted a Cybersecurity Incident Exercise with several municipal and state DOT participants.

The cybersecurity incident exercise mechanics, outlined below, focused on testing the proposed process to ensure gap coverage and ease of use/understanding of the proposed protocols and procedures. Through reviewing participant responses and activities from the exercise, the research team was able to identify areas in which the developed cybersecurity incident communication protocols were successful and areas of improvements. Specifics on the design and execution of the exercise are detailed in the "Transportation Cybersecurity Incident Response and Management Framework: Cybersecurity Incident Exercise Summary Report," (FHWA-JPO-21-850).

The key findings and lessons learned from the execution of the cyber incident exercise are summarized in the following sections.

Differences in Score Due to Changes in Communication Process

Selection criteria for the participants invited to this exercise were individuals with backgrounds in traffic engineering, operations, and management of TMCs. Participants had some general cybersecurity knowledge or awareness however none had a title or background in cybersecurity or direct experience in handling cyber incidents within their organization.

Through the interactions during first exercise of the Cyber Incident Exercise, the research team was able to discern what 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 versus communicating the incident. Response activities 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.

During this initial exercise, multiple turns between participants passed in the exercise where information was either not being shared or not reaching all anticipated reporting levels. While responding with mitigating activities realizes steps within a cyber incident response, for this focused exercise, these activities were considered an assumed parallel process and out of scope. 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 CISO (opposed to one turn internally to TMC). As a result of participants' delay in beginning the communication exchange process and missing some important information sharing actions (i.e., share vulnerability report), the scores received by participants for this exercise were low. This exercise resulted in the following scores, where the highest score available is 67 points and the lowest score is 0 points (A full breakdown of the scores available in Appendix E):

- Municipal IOO—3 points.
- Fusion 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 step of "executing 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, where the highest score available is 67 points and the lowest score is 0 points (full breakdown of scores available in Appendix E):

- Municipal IOO—6 points.
- Fusion Center / 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 share information more effectively, 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 consider any pre-coordination that may be necessary (contacting a 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 which roles have what level of authority to share information and ensure all resources necessary to the developed processes are available 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 compiled below:

- 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 LE—Participant noted that they were hesitant to reach out because we want absolute certainty in the information they have. 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.

Proposed Solution Summary

To develop a framework to improve communication regarding transportation cybersecurity incidents, multiple steps were necessary. Each of the stakeholder types and information sharing resources were identified, and with a common vocabulary, were provided with recommendations and protocols on how to effectively share incident information. Upon testing these protocols, multiple lessons learned and improvements to incorporate were noted, but the stakeholders ultimately improved both the rate and content of their information sharing.

Chapter 6. Conclusion

The objective of this project was to develop a framework (Appendix A) for communication and information sharing with transportation roadway stakeholders when detecting and responding to a cyber-attack or vulnerability that spans across devices or other sectors. This objective was achieved through understanding the current environment in transportation cybersecurity information sharing, developing a set of protocols to improve the communication process, and finally testing the developed protocols in a cyber incident exercise to ensure further gaps were not present.

Through the successful completion of these efforts, the following key takeaways were observed:

- To best facilitate effective information sharing, state agencies and other transportation stakeholders should reach out to Fusion Centers to begin the information sharing process. The amount of connections and law enforcement capabilities available to Fusion Centers provides a simple pathway for state agencies and other transportation stakeholders to widely share cyber incident information.
- On top of the recommended use cases and process improvements for each information sharing organizations, it is recommended that each municipal and/or state IOO both:
  - Maintain a working relationship with their state CISO or CIO, such that in the case of a cyber incident, the state will be readily available to assist.
  - Maintain a working relationship with their Primary and, where available, Recognized, Fusion Center(s).

Through the development and testing of the procedures, we were able to produce an effective framework for cybersecurity incident information sharing. As shown in the results of the incident exercise, response times and the content of responses (i.e., vulnerability reporting) were improved by each of the participants. By incorporating lessons learned from the exercise, we were able to further improve these protocols of the framework in terms of understandability and effectiveness. Though there is extensive work to be completed in improving cyber incident response communication, like future incident exercises and potential outreach with findings from this report, this project presents a baseline framework which can assist transportation roadway stakeholders when detecting and responding to a cyber-attack or vulnerability.

Appendix A. Recommended Communication Flows

Use Case 1—Municipal Infrastructure Owner Operator

A municipal IOO usually discovers a vulnerability in an OT device.

The goals of the procedures shown in Table 1 and Table 2 and information flows in Figure 6 and Figure 7 below are to make sure all of the relevant stakeholders received this information reliably and quickly.

Table 1. UC1-S1: Municipal infrastructure owner operator procedures for non-active attack use case.

Use Case	Municipal IOO Procedures for Non-Active Attack Use Case	
Scenario ID & Title	UC1-S1: Municipal IOO Procedures for Non-Active Attack Use Case	
Scenario Objective	Make sure all the relevant stakeholders received this information reliably and quickly	
Operational Event(s)	Discover vulnerability in advance of active attack	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	• Assumed that vulnerability report is generated municipal by IOO. • The discovery is during performance of normal business and not due to an active attack. • The discovery is not due to maintenance issues, but a vulnerability due to how a device is designed or used in a nominal condition.	

Use Case	Municipal IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Municipal IOO	Municipal IOO confirms vulnerability and that it is NOT part of an active cyber-attack.	
1.1	Municipal IOO	Municipal IOO executes their cybersecurity IMP[1], also known as incident response plan or emergency management plan, or other cybersecurity vulnerability management procedures.	Note: Not all Municipal IOOs have an explicit IMP. An IMP or other reporting procedures referenced include generating a summary on the vulnerability (See Vulnerability Reporting Template for more information) and instructions for contacting workers or subcontractors who perform safety-critical roadway and maintenance operations.
1.1.1	Municipal IOO	Municipal IOO follows cybersecurity incident response procedures to quarantine affected equipment for mitigation and recovery processes.	
1.1.2	Municipal IOO	Municipal IOO follows cybersecurity incident response procedures, where available, or seeks upper management approval to inform system integrators and internal contractors who perform safety-critical roadway and maintenance operations (This includes IT and OT teams) of vulnerability information.	Where a Municipal IOO does not have formal procedures directing when incident information can be shared outside their department or organization, they need to see management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the IOO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact. See Vulnerability Reporting Template for more information.
1.1.3	Municipal IOO	Municipal IOO reports vulnerability to the equipment manufacturer (not contractor/reseller).	

Use Case	**Municipal IOO Procedures for Non-Active Attack Use Case**		
Step	**Actor**	**Key Action**	**Comments**
1.1.3.1	Equipment Manufacturer	Once the equipment manufacturer is informed of the issue, ideally, they will work with IOO to develop a security patch and continue their response by developing a software update patching all affected systems.	Note: This is behavior not guaranteed, but a desired outcome of contacting the equipment manufacturer.
2	Municipal IOO	**If** the Municipal IOO has a Municipal CISO:	**Else** go to Step 3.
2.1	Municipal IOO	Municipal IOO reports non-active cyber incident to Municipal CISO (See Figure 6 for more information).	Municipal IOO will also provide list of safety critical contractors and system integrators to the Municipal CISO/CIO.
2.2	Municipal CISO	Municipal CISO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability.
2.3	Municipal CISO	Municipal CISO shares authorized vulnerability information with State CISO.	Where a Municipal CISO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the CISO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact. See Vulnerability Reporting Template for more information.
2.3.1	State CISO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability and identify known mitigation measures.

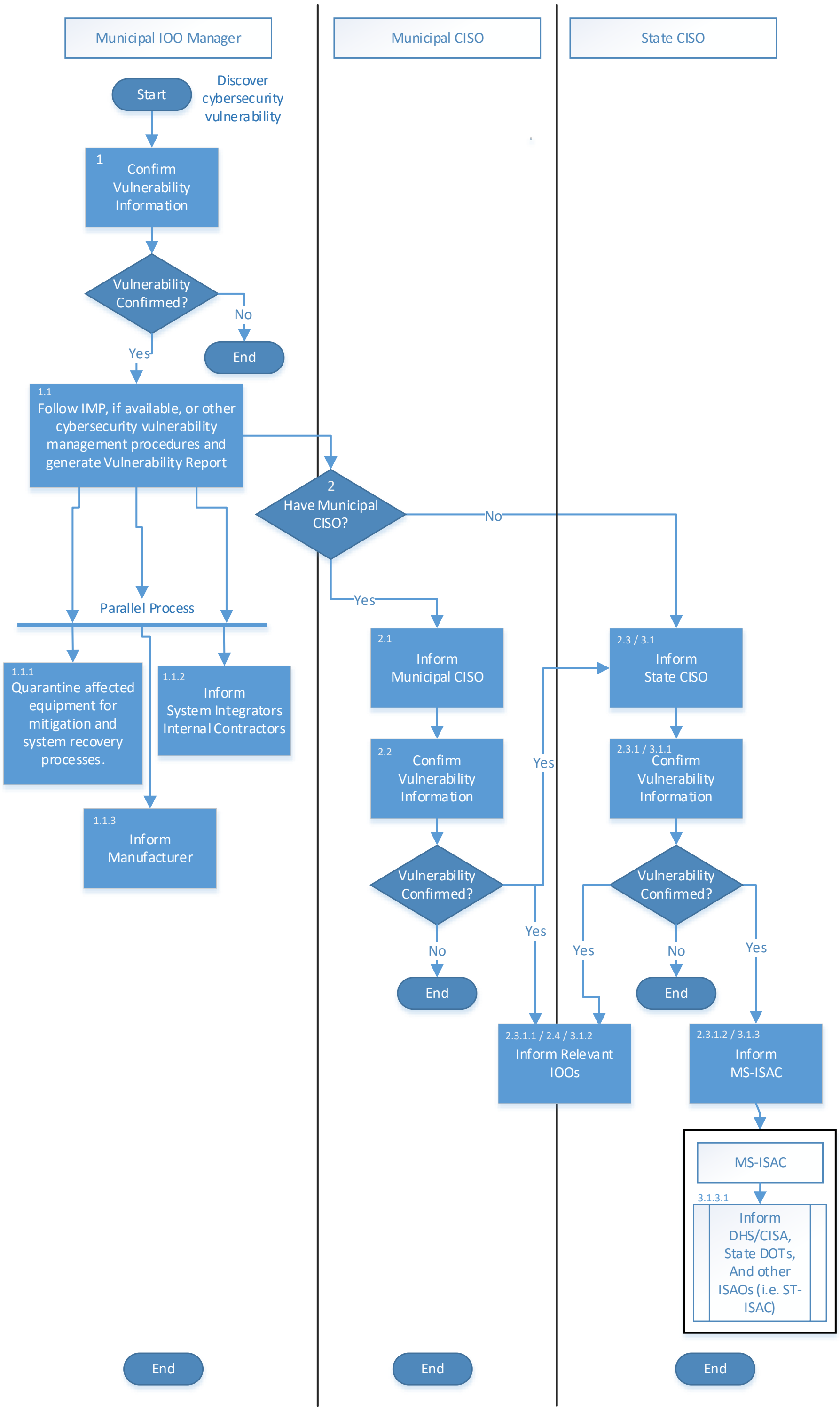
Use Case	Municipal IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.3.1.1	State CISO	State CISO shares information with other municipal/state CISOs and IOOs within their area of responsibility.	Where a State CISO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the CISO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact.
2.3.1.2	State CISO	State CISO shares vulnerability report with MS-ISAC.	
2.4	Municipal CISO	Municipal CISO shares information with other IOOs within their area of responsibility.	
3	Municipal IOO	**Else** Municipal IOO does not have a Municipal CISO.	
3.1	Municipal IOO	Municipal IOO reports non-active cyber incident to State CISO/CIO (See 0 for more information).	Municipal IOO will also provide list of safety critical contractors and system integrators to the Municipal CISO/CIO.
3.1.1	State CISO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability and identify known mitigation measures.
3.1.2	State CISO	State CISO/CIO shares vulnerability report to other IOOs within their boundaries of responsibility.	
3.1.3	State CISO	State CISO shares vulnerability report with MS-ISAC.	

Use Case	Municipal IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
3.1.3.1	MS-ISAC	MS-ISAC shares the vulnerability report with DHS/CISA and across ISAOs[2], including other ISAO members in accordance with ISAO 300-1: Introduction to Information Sharing.	Vulnerability reporting includes the following details to the best of the IOO's ability: Description of the vulnerability (included affected device) Initial assessment of severity Point of contact
3.1.3.1.1	MS-ISAC	MS-ISAC shares the vulnerability report with related ISAO(s) covering this vulnerability.	
3.1.3.1.2	MS-ISAC	MS-ISAC shares vulnerability report to DHS/CISA either via United States Cyber Emergency Response Team (U.S.-CERT), Industrial Control Systems U.S.-CERT (ICS-CERT), NCCIC, or the reporting mechanism available at the time	

Note: All identified actors have information regarding the discovered vulnerability.

[1] Incident Management Plan—The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information systems(s).

[2] Information Sharing and Analysis Organizations—An entity or collaboration created or employed by public- or private sector organizations for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability (NIST SP 800-150).


Municipal IOO Manager
Municipal CISO
State CISO
Start
Discover cybersecurity vulnerability
1 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
1.1 Follow IMP, if available, or other cybersecurity vulnerability management procedures and generate Vulnerability Report
2 Have Municipal CISO?
No
Yes
Parallel Process
1.1.1 Quarantine affected equipment for mitigation and system recovery processes.
1.1.2 Inform System Integrators Internal Contractors
1.1.3 Inform Manufacturer
2.1 Inform Municipal CISO
2.2 Confirm Vulnerability Information
Vulnerability Confirmed?
Yes
Yes
No
End
2.3 / 3.1 Inform State CISO
2.3.1 / 3.1.1 Confirm Vulnerability Information
Vulnerability Confirmed?
Yes
No
Yes
End
2.3.1.1 / 2.4 / 3.1.2 Inform Relevant IOOs
2.3.1.2 / 3.1.3 Inform MS-ISAC
MS-ISAC
3.1.3.1 Inform DHS/CISA, State DOTs, And other ISAOs (i.e. ST-ISAC)
End
End
End

Source: FHWA

Figure 6. Flowchart. UC1-S1: Municipal infrastructure owner operator procedures for non-active attack use case.

Table 2. UC1-S2: Municipal infrastructure owner operator procedures for active attack use case.

Use Case	Municipal IOO Procedures for Active Attack Use Case	
Scenario ID & Title	UC1-S2: Municipal IOO Procedures for Active Attack Use Case	
Scenario Objective	Make sure all of the relevant stakeholders received this information reliably and quickly	
Operational Event(s)	Discover vulnerability during active attack	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	• Assumed that vulnerability report is generated municipal by IOO. • A municipal IOO discovers a vulnerability as part of an active cyber-attack against a Municipal IOO.	

Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Municipal IOO	Municipal IOO confirms vulnerability and that it is part of an active cyber-attack.	

Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1.1	Municipal IOO	Municipal IOO executes their IMP, if available, or other cybersecurity incident response procedures for an active cyber-attack.	Note: Not all Municipal IOOs have an explicit IMP. IMP or other reporting procedures referenced include generating a summary on the vulnerability (See Vulnerability Reporting Template for more information) and instructions for contacting workers or subcontractors who perform safety-critical roadway and maintenance operations.
1.1.1	Municipal IOO	Municipal IOO follows cybersecurity incident response procedures to quarantine affected equipment for recovery and potential investigation process by LE.	
1.1.2	Municipal IOO	Municipal IOO follows cybersecurity incident response procedures. Where available or seeks upper management approval to begin informing system integrators and internal contractors who perform safety-critical roadway and maintenance operations (this includes IT and OT teams) of vulnerability information.	Where a Municipal IOO does not have formal procedures directing when incident information can be shared outside their department or organization, they need to seek management approval so that cyber incident mitigation and response can move forward.
1.1.3	Municipal IOO	Municipal IOO reports vulnerability to the equipment manufacturer (not contractor/reseller).	

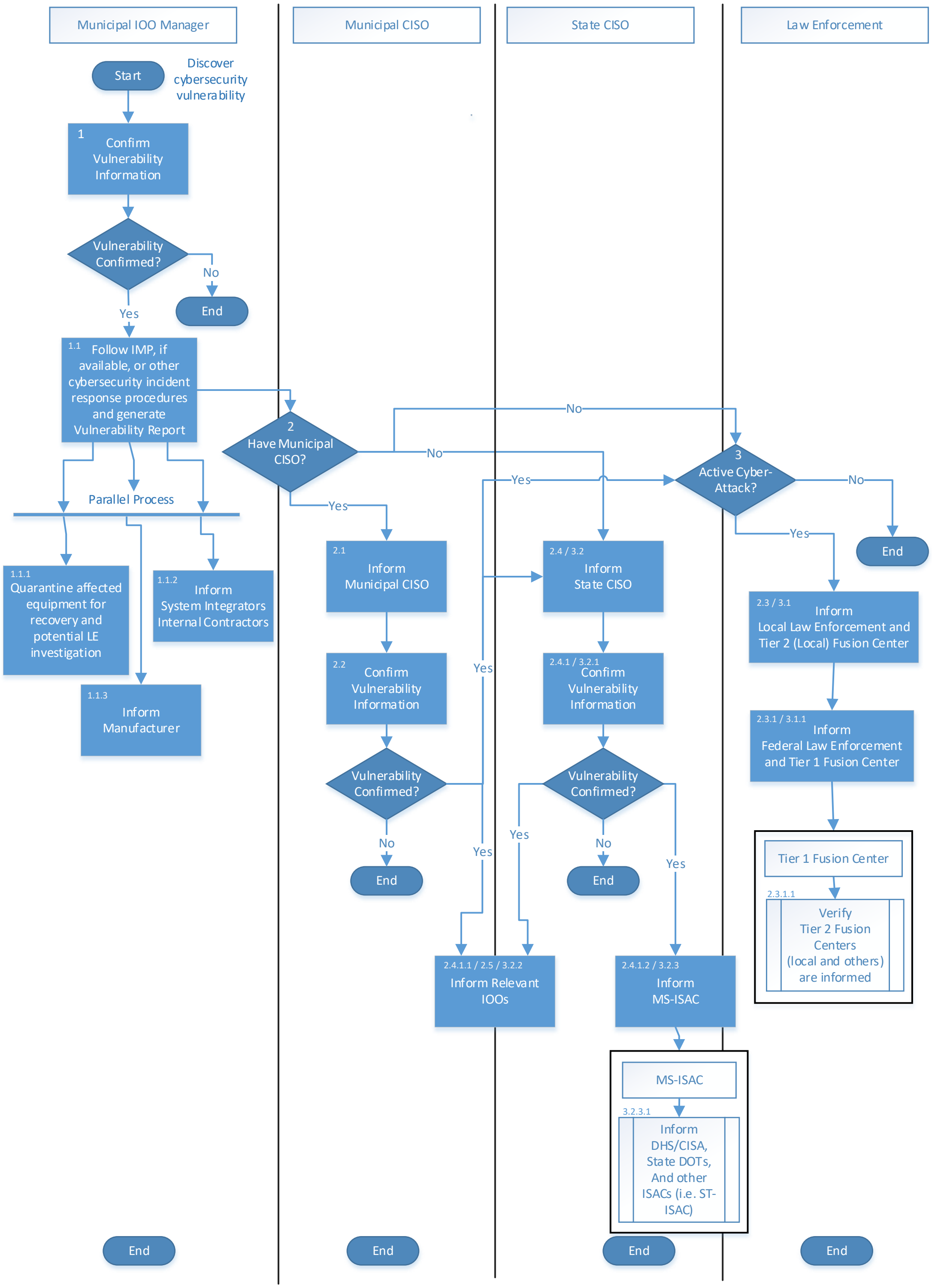
Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1.1.3.1	Equipment Manufacturer	Once the equipment manufacturer is informed of the active issue, ideally, they will start by coordinating with the IOO to develop an initial security patch and continue their response by developing a software update patching all affected systems.	Note: This is behavior not guaranteed, but a desired outcome of contacting the equipment manufacturer.
2	Municipal IOO	**If** the Municipal IOO has a Municipal CISO:	**Else** go to Step 3.
2.1	Municipal IOO	Municipal IOO reports active cyber incident to Municipal CISO (See Vulnerability Reporting Template for more information).	Vulnerability reporting includes the following details to the best of the IOO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact. Municipal IOO will also provide list of safety critical contractors and system integrators to the Municipal CISO/CIO.
2.2	Municipal CISO	Municipal CISO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability.
2.3	Municipal CISO	Municipal CISO contacts local LE and Recognized (local) Fusion Center, if one exists for municipality and provides the vulnerability report.	

Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.3.1	Local LE	Local LE will involve Federal LE as necessary and contact Primary (state) Fusion Center to inform them of the vulnerability.	
2.3.1.1	Fusion Center	Primary Fusion Center verifies that vulnerability report has been shared with Recognized Fusion Center(s).	
2.3.1.2	Fusion Center	Fusion Centers provide incident management support to the municipal IOO and share vulnerability information with DHS/CISA and other agencies.	
2.4	Municipal CISO	Municipal CISO shares information with State CISO.	Where a Municipal CISO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the CISO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact.
2.4.1	State CISO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability and identify known mitigation measures.

Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.4.1.1	State CISO	State CISO shares information with other municipal/state CISOs and IOOs within their area of responsibility.	Where a State CISO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the CISO’s ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact.
2.4.1.2	State CISO	State CISO shares vulnerability report with MS-ISAC.	
2.5	Municipal CISO	Municipal CISO shares information with other IOOs within their area of responsibility.	
3	Municipal IOO	**Else** Municipal IOO does not have a Municipal CISO:	
3.1	Municipal IOO	Municipal IOO reports active cyber incident to local LE and Recognized (local) Fusion Center, if one exists for municipality and provides the vulnerability report.	
3.1.1	Local LE	Local LE will involve Federal LE as necessary and contact Primary (state) Fusion Center to inform them of the vulnerability.	

Use Case	Municipal IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
3.2	Municipal IOO	Municipal IOO reports active cyber incident to State CISO/CIO (See Figure 7 for more information).	Municipal IOO will also provide list of safety critical contractors and system integrators to the State CISO/CIO.
3.2.1	State CISO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability and identify known mitigation measures.
3.2.2	State CISO	State CISO/CIO shares vulnerability report to other IOOs within their boundaries of responsibility.	
3.2.3	State CISO	State CISO shares vulnerability report with MS-ISAC.	
3.2.3.1	MS-ISAC	MS-ISAC shares the vulnerability report with DHS/CISA and across ISAOs, including other ISAO members in accordance with ISAO 300-1: Introduction to Information Sharing.	Report includes the following details to the best of the IOO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact
3.2.3.1.1	MS-ISAC	MS-ISAC shares the vulnerability report with related ISAO(s) covering this vulnerability.	
3.2.3.1.2	MS-ISAC	MS-ISAC shares vulnerability report to DHS/CISA either via U.S.-CERT, ICS-CERT, NCCIC, or the reporting mechanism available at the time.	

Note: All identified actors have information regarding the discovered vulnerability.


Municipal IOO Manager
Municipal CISO
State CISO
Law Enforcement
Start
Discover cybersecurity vulnerability
1 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
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
2 Have Municipal CISO?
No
Yes
2.1 Inform Municipal CISO
2.2 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
Yes
No
Yes
2.4 / 3.2 Inform State CISO
2.4.1 / 3.2.1 Confirm Vulnerability Information
Vulnerability Confirmed?
Yes
No
End
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 7. Flowchart. UC1-S2: Municipal infrastructure owner operator procedures for active attack use case.

Use Case 2—State IOO

Like the municipal IOO, when a state IOO discovers a vulnerability in their system, they will reach out to their equipment manufacturers/software vendors and municipal LE using a vulnerability report.

During this scenario, the following procedures in Table 3 and Table 4 and information flows in Figure 8 and Figure 9 would be followed by an IOO.

Table 3. UC2-S1: State infrastructure owner operator procedures for non-active attack use case.

<table>
<tr><th>Use Case</th><th colspan="2">State IOO Procedures for Non-Active Attack Use Case</th></tr>
<tr><td>Scenario ID &amp; Title</td><td colspan="2">UC2-S1: State IOO Procedures for Non-Active Attack Use Case</td></tr>
<tr><td>Scenario Objective</td><td colspan="2">Make sure all of the relevant stakeholders received this information reliably and quickly</td></tr>
<tr><td>Operational Event(s)</td><td colspan="2">Discover vulnerability in advance of active attack</td></tr>
<tr><td rowspan="7">Actor(s)</td><th>Actor</th><th>Role</th></tr>
<tr><td>Law Enforcement</td><td>Provides mitigation information and possible investigation if needed</td></tr>
<tr><td>DHS/CISA</td><td>Cyber Information Sharing Agency</td></tr>
<tr><td>MS-ISAC</td><td>Multi-state ISAC, large membership in transportation</td></tr>
<tr><td>State/Municipal CISO</td><td>Chief Information Security Officer, responsible for the implementation of information security policy</td></tr>
<tr><td>State/Municipal IOO</td><td>Infrastructure Owner Operators, interact with end devices</td></tr>
<tr><td>Equipment Manufacturer</td><td>Designed and developed the affected device used by IOO</td></tr>
<tr><td>Pre-conditions</td><td colspan="2">• Assumed that vulnerability report is generated by State IOO.
• The discovery is during performance of normal business and not due to an active attack.
• The discovery is not due to maintenance issues, but a vulnerability due to how a device is designed or used in a nominal condition.</td></tr>
</table>

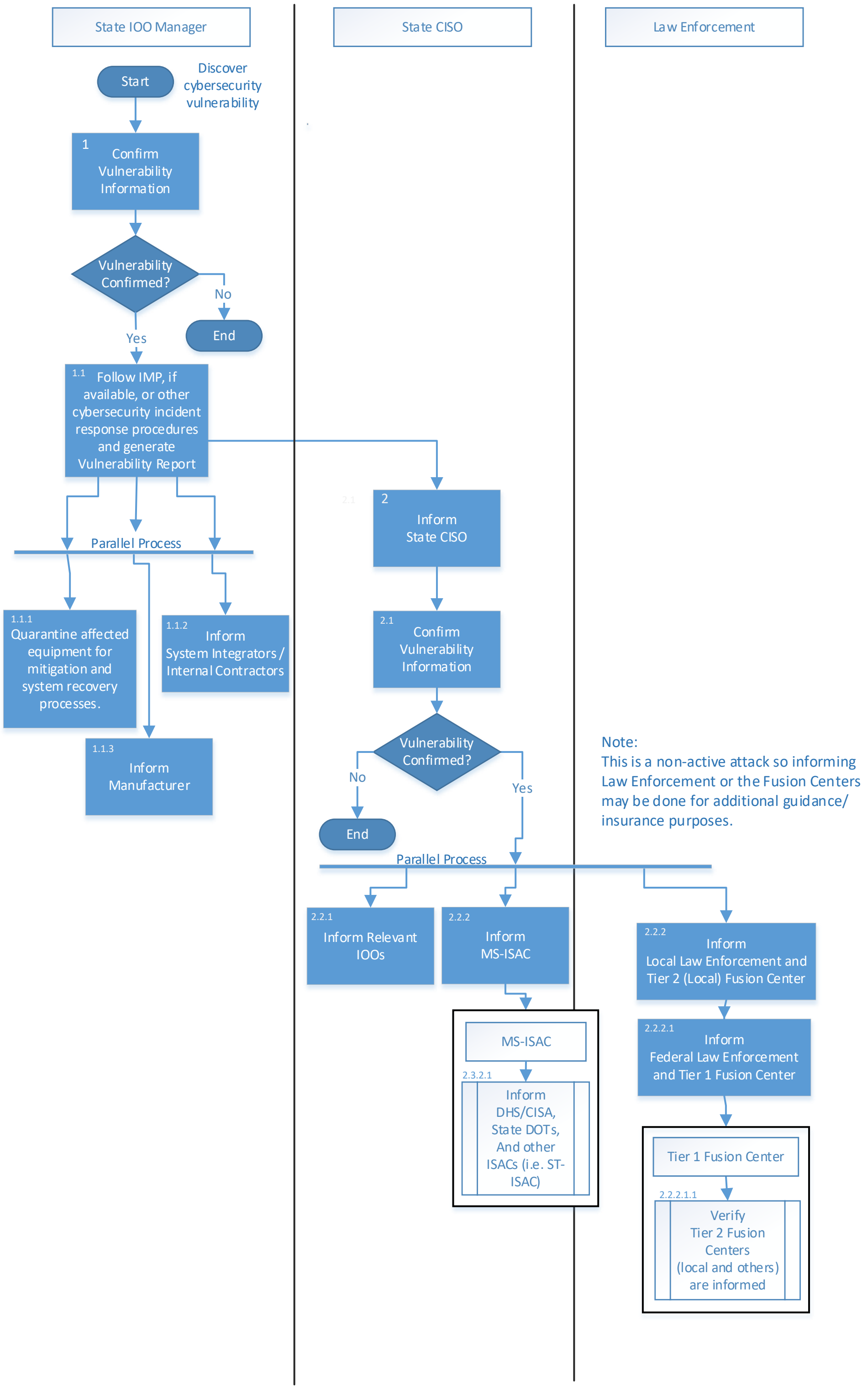
Use Case	State IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	State IOO	State IOO confirms vulnerability and that it is **NOT** part of an active cyber-attack.	
1.1	State IOO	State IOO executes their IMP, also known as incident response plan or emergency management plan.	Note: Not all State IOOs have an explicit IMP. An IMP or other reporting procedures referenced include generating a summary on the vulnerability and instructions for contacting workers or subcontractors who perform safety-critical roadway and maintenance operations. If the vulnerability could impact safety, this includes instructions for contacting workers or subcontractors who perform safety-critical roadway and maintenance operations.
1.1.1	State IOO	State IOO follows cybersecurity incident response procedures to quarantine affected equipment for mitigation and recovery processes.	

Use Case	State IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1.1.2	State IOO	State IOO follows cybersecurity incident response procedures for informing system integrators and internal contractors who perform safety-critical roadway and maintenance operations (This includes IT and OT teams) of vulnerability information.	Where a State IOO does not have formal procedures directing when incident information can be shared outside their department or organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the IOOs ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact The information in the vulnerability report will contain the previously identified data requirements to provide the minimum information needed to assist stakeholders in cyber incident information exchange (See Vulnerability Reporting Template for more information).
1.1.3	State IOO	State IOO reports vulnerability to the equipment manufacturer (not contractor/reseller).	

Use Case	State IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1.1.3.1	Equipment Manufacturer	Once the equipment manufacturer is informed of the issue, ideally, they will work with IOO to develop a security patch and continue their response by developing a software update patching all affected systems.	Note: This is behavior not guaranteed but a desired outcome of contacting the equipment manufacturer.
2	State IOO	State IOO reports non-active cyber incident to State CISO/CIO (See Figure 8 for more information).	State IOO will also provide list of safety critical contractors and system integrators to the State CISO/CIO.
2.1	State CISO/CIO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability and identify known mitigation measures.
2.2	-	The following activities would then be executed in parallel:	
2.2.1	State CISO/CIO	State CISO/CIO shares vulnerability report with other affected Municipal/State IOO within their geographical boundaries of responsibility.	Where a State CISO/CIO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the CISO's ability: Description of the vulnerability (included affected device) Initial assessment of severity Point of contact.

Use Case	State IOO Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.2.2	State CISO/CIO	State CISO/CIO shares vulnerability report with local LE and Recognized (local) Fusion Center, if one exists for geographical area.	As this is not an active incident, this activity may be done for additional guidance and insurance purposes.
2.2.2.1	Local LE	Local LE will involve Federal LE as necessary and contact Primary (state) Fusion Center with vulnerability report.	
2.2.2.1.1	Fusion Center	Primary Fusion Center verify vulnerability report has been shared with Recognized Fusion Centers.	
2.2.2.1.2	Fusion Center	Fusion Centers then share vulnerability report with DHS/CISA and provide incident management materials/support to the state IOO.	
2.2.3	State CISO/CIO	State CISO/CIO shares vulnerability report with MS-ISAC.	
2.2.3.1	MS-ISAC	The MS-ISAC shares the vulnerability report with DHS/CISA and across ISAO(s), including other ISAO members in accordance with ISAO 300-1: Introduction to Information Sharing.	
2.2.3.1.1	MS-ISAC	MS-ISAC shares vulnerability report with related ISAO(s) covering the vulnerability.	
2.2.3.1.2	MS-ISAC	MS-ISAC shares to DHS/CISA either via U.S.-CERT, ICS-CERT, NCCIC, or the reporting mechanism available at the time.	

Note: All identified actors have information regarding the discovered vulnerability.


State IOO Manager
State CISO
Law Enforcement
Start
Discover cybersecurity vulnerability
1 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
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 mitigation and system recovery processes.
1.1.2 Inform System Integrators / Internal Contractors
1.1.3 Inform Manufacturer
2 Inform State CISO
2.1 Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
Parallel Process
2.2.1 Inform Relevant IOOs
2.2.2 Inform MS-ISAC
MS-ISAC
2.3.2.1 Inform DHS/CISA, State DOTs, And other ISACs (i.e. ST-ISAC)
2.2.2 Inform Local Law Enforcement and Tier 2 (Local) Fusion Center
2.2.2.1 Inform Federal Law Enforcement and Tier 1 Fusion Center
Tier 1 Fusion Center
2.2.2.1.1 Verify Tier 2 Fusion Centers (local and others) are informed

Note:
This is a non-active attack so informing Law Enforcement or the Fusion Centers may be done for additional guidance/ insurance purposes.

Source: FHWA

Figure 8. Flowchart. UC2-S1: State infrastructure owner operator procedures for non-active attack use case.

Table 4. UC2-2: State infrastructure owner operator procedures for active attack use case.

Use Case	State IOO Procedures for Active Attack Use Case	
Scenario ID & Title	UC2-S2: State IOO Procedures for Active Attack Use Case	
Scenario Objective	Make sure all of the relevant stakeholders received this information reliably and quickly	
Operational Event(s)	Discover vulnerability during of active attack	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	• Assumed that vulnerability report is generated by State IOO. • The discovery is during an active attack.	

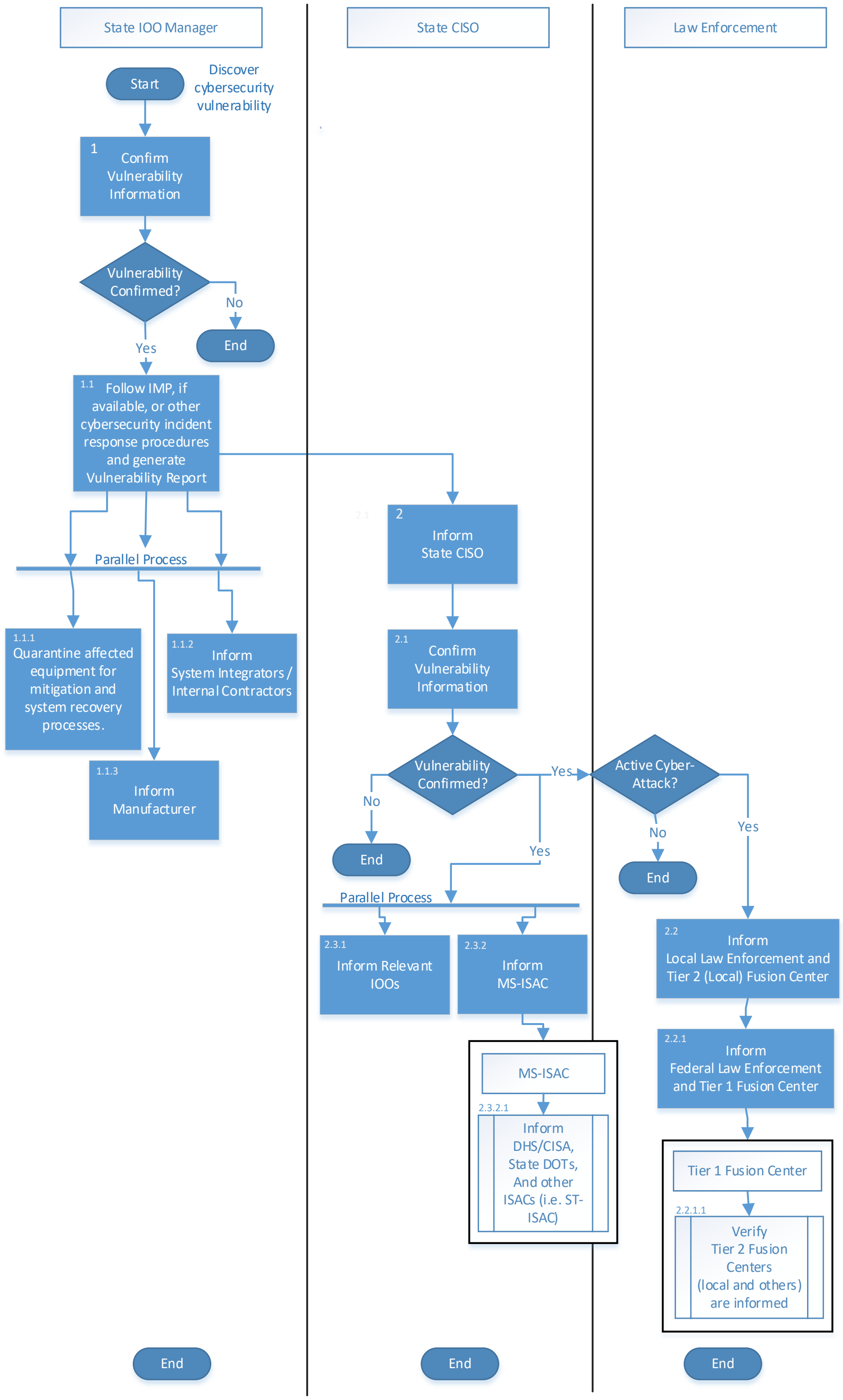
Use Case	State IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	State IOO	State IOO confirms vulnerability and that it is part of an active cyber-attack.	
1.1	State IOO	State IOO executes their IMP, also known as incident response plan or emergency management plan.	Note: Not all State IOOs have an explicit IMP. IMP or other reporting procedures referenced include generating a summary on the vulnerability and instructions for contacting workers or subcontractors who perform safety-critical roadway and maintenance operations.

Use Case	State IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1.1.1	State IOO	State IOO follows cybersecurity incident response procedures to quarantine affected equipment for mitigation and recovery processes.	
1.1.2	State IOO	State IOO follows cybersecurity incident response procedures for informing system integrators and internal contractors who perform safety-critical roadway and maintenance operations (This includes IT and OT teams) of vulnerability information.	Where a State IOO does not have formal procedures directing when incident information can be shared outside their department or organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the IOO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact. The information in the vulnerability report will also contain the previously identified data requirements to provide the minimum information needed to assist stakeholders in cyber incident information exchange. See 0 for more information.
1.1.3	State IOO	State IOO reports vulnerability to the equipment manufacturer (not contractor/reseller).	
1.1.3.1	Equipment Manufacturer	Once the equipment manufacturer is informed of the active issue, ideally, they will start by coordinating with the IOO to develop an initial security patch and continue their response by developing a software update patching all affected systems.	Note: This is behavior not guaranteed, but a desired outcome of contacting the equipment manufacturer.

Use Case	State IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2	State IOO	State IOO contacts State CISO/CIO with a vulnerability report (See Vulnerability Reporting Template for more information).	State IOO will also provide list of safety critical contractors and system integrators to the State CISO/CIO.
2.1	State CISO/CIO	State CISO/CIO confirms vulnerability information.	This may include comparing initial report from IOO with known CVEs to see if others have reported the same vulnerability.
2.2	State CISO/CIO	State CISO/CIO contacts local LE and Recognized (local) Fusion Center, IF one exists for municipality and provides the vulnerability report.	Where a State CISO does not have formal procedures directing when incident information can be shared outside their organization, they need to seek management approval so that cyber incident mitigation and response can move forward. Vulnerability reporting includes the following details to the best of the IOO's ability: • Description of the vulnerability (included affected device) • Initial assessment of severity • Point of contact.
2.2.1	Local LE	Local LE will involve Federal LE as necessary and contact Primary (state) Fusion Center to inform them of the vulnerability.	
2.2.1.1	Fusion Center	Primary Fusion Center verifies that vulnerability report has been shared with Recognized Fusion Centers.	
2.2.1.2	Fusion Center	Fusion Centers provide incident management support to the municipal IOO and share vulnerability information with DHS/CISA and other agencies.	

Use Case	State IOO Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.3	State CISO/CIO	State CISO/CIO then shares vulnerability report in parallel with the following agencies:	
2.3.1	State CISO/CIO	Other affected IOOs within their geographical boundaries of responsibility.	
2.3.2	State CISO/CIO	State CISO/CIO shares vulnerability report with MS-ISAC.	
2.3.2.1	MS-ISAC	The MS-ISAC shares the vulnerability report with DHS/CISA and across ISAO(s), including other ISAO members in accordance with ISAO 300-1: Introduction to Information Sharing.	

Note: All identified actors have information regarding the discovered vulnerability.


State IOO Manager
State CISO
Law Enforcement
Start
Discover cybersecurity vulnerability
1
Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
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 mitigation and system recovery processes.
1.1.2
Inform System Integrators / Internal Contractors
1.1.3
Inform Manufacturer
End
2
Inform State CISO
2.1
Confirm Vulnerability Information
Vulnerability Confirmed?
No
End
Yes
Yes
Parallel Process
2.3.1
Inform Relevant IOOs
2.3.2
Inform MS-ISAC
MS-ISAC
2.3.2.1
Inform DHS/CISA, State DOTs, And other ISACs (i.e. ST-ISAC)
End
Active Cyber-Attack?
No
End
Yes
2.2
Inform Local Law Enforcement and Tier 2 (Local) Fusion Center
2.2.1
Inform Federal Law Enforcement and Tier 1 Fusion Center
Tier 1 Fusion Center
2.2.1.1
Verify Tier 2 Fusion Centers (local and others) are informed
End

Source: FHWA

Figure 9. Flowchart. UC2-S2: State infrastructure owner operator procedures for active attack use case.

Use Case 3—Law Enforcement

In this use case, a Federal or local law enforcement agency discovers a vulnerability. The sharing is facilitated using vulnerability reports (See Appendix B. Vulnerability Reporting Template for an example) to be prepared for those directly affected and delivered immediately.

The following shown in Table 5 and Table 6 and information flows in Figure 10 and Figure 11 capture the procedures for a vulnerability sharing effort from law enforcement agencies:

Table 5. UC3-S1: Law enforcement procedures for non-active attack use case.

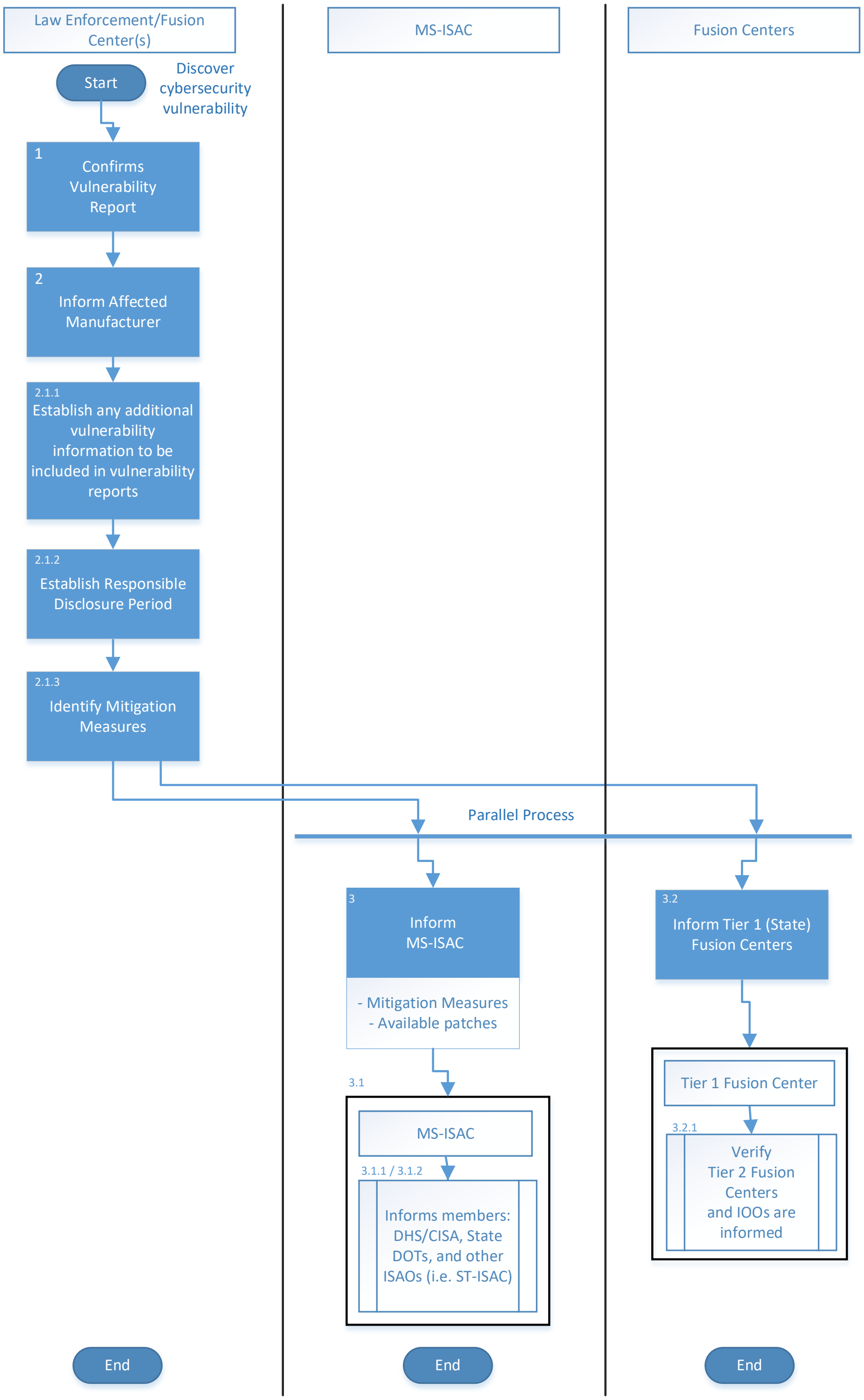
Use Case	Law Enforcement Procedures for Non-Active Attack Use Case	
Scenario ID & Title	UC3-S1: Law Enforcement Procedures for Non-Active Attack Use Case	
Scenario Objective	Make sure all of the relevant stakeholders receive this information reliably and quickly	
Operational Event(s)	Discover vulnerability in advance of active attack	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	Law Enforcement agency receives a vulnerability report in advance of any active exploit.	

Use Case	Law Enforcement Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Law Enforcement	Law Enforcement agency confirms vulnerability and that it is NOT part of an active cyber-attack.	

Use Case	Law Enforcement Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2	Law Enforcement	Law Enforcement agency shares vulnerability report with affected equipment manufacturer.	Note: Information released may be limited due to criminal investigation.
2.1	Law Enforcement	Law Enforcement performs the following additional steps:	
2.1.1	Law Enforcement	Establish any additional vulnerability information to be included in vulnerability reports (See Vulnerability Reporting Template for more information).	
2.1.2	Law Enforcement	Establish responsible disclosure period.	
2.1.3	Law Enforcement	Identify interim mitigation measures, if possible and provide this to equipment manufacturer.	
3	Law Enforcement	Law Enforcement agency shares vulnerability report with MS-ISAC and additional information as appropriate.	Additional information includes: • Mitigation measures and procedures. • Available patches to be installed on affected devices.
3.1	MS-ISAC	MS-ISAC pass vulnerability report to:	
3.1.1	MS-ISAC	MS-ISAC members, who may include State and Municipal CISOs/CIOs.	
3.1.1.1	State CISO	State CISO shares vulnerability report with other affected Municipal or State IOO within their geographical boundaries of responsibility.	
3.1.2	MS-ISAC	Other ISAOs, such as ST-ISAC, and with various Government entities in accordance with ISAO 300-1: Introduction to Information Sharing.	
3.2	Law Enforcement	Law Enforcement agency shares vulnerability report with Primary (State) Fusion Centers.	

Use Case	Law Enforcement Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
3.2.1	Fusion Center	Primary Fusion Centers will flow information to Recognized Fusion Centers and share vulnerability report with IOOs within their geographical area of responsibility.	

Note All identified actors have information regarding the discovered vulnerability.


Law Enforcement/Fusion Center(s)
MS-ISAC
Fusion Centers
Start
Discover cybersecurity vulnerability
1
Confirms Vulnerability Report
2
Inform Affected Manufacturer
2.1.1
Establish any additional vulnerability information to be included in vulnerability reports
2.1.2
Establish Responsible Disclosure Period
2.1.3
Identify Mitigation Measures
Parallel Process
3
Inform MS-ISAC
- Mitigation Measures
- Available patches
3.1
MS-ISAC
3.1.1 / 3.1.2
Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
3.2
Inform Tier 1 (State) Fusion Centers
Tier 1 Fusion Center
3.2.1
Verify Tier 2 Fusion Centers and IOOs are informed
End
End
End

Source: FHWA

Figure 10. Flowchart. UC3-S1: Law enforcement procedures for non-active attack use case.

Table 6. UC3-S2: Law enforcement use case active attack.

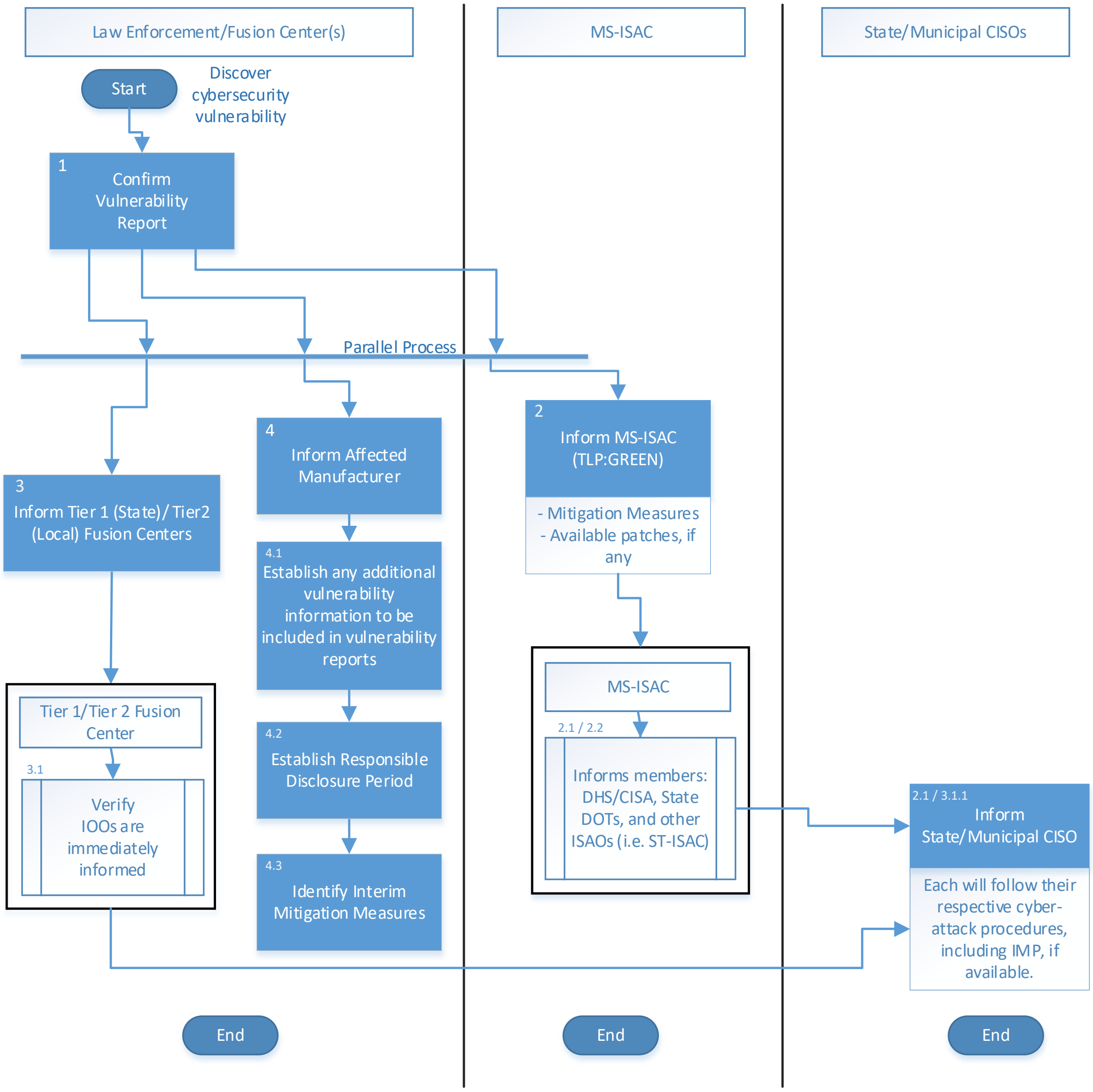
Use Case	Law Enforcement Procedures for Active Attack Use Case	
Scenario ID & Title	UC3-S2: Law Enforcement Procedures for Active Attack Use Case	
Scenario Objective	Make sure all the relevant stakeholders received this information reliably and quickly	
Operational Event(s)	Law Enforcement receives a vulnerability report during an active cyber-attack	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	Law Enforcement receives a vulnerability report during an active attack from a security researcher.	

Use Case	Law Enforcement Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Law Enforcement	Law Enforcement agency confirms vulnerability and that it is part of an active cyber-attack.	
2	Law Enforcement	Law Enforcement agency shares immediate mitigation information (Classified as TLP: Green) with MS-ISAC.	Immediate mitigation information contains actionable measures to block or effect active cyber-attack. This information also contains information on vulnerable user characteristics and system characteristics.

Use Case	Law Enforcement Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.1	MS-ISAC	MS-ISAC contacts State CISOs and provides vulnerability report and mitigation information.	
2.1.1	MS-ISAC	As developing mitigation information becomes available, MS-ISAC will immediately share with all members.	
2.2	MS-ISAC	MS-ISAC shares vulnerability report with related ISAO covering this vulnerability.	
3	Law Enforcement	Law Enforcement agency shares immediate mitigation information with all Primary and Recognized Fusion Centers.	
3.1	Fusion Center	Primary and Recognized Fusion Centers immediately shares mitigation information with all Municipal and State CISOs within their geographical area of responsibility.	
3.1.1	Municipal/State CISOs	Each will execute their respective cyber-attack procedures, including IMP, if available.	They will continue to coordinate with law enforcement as part of the mitigation and criminal investigation process.
4	Law Enforcement	Law Enforcement shares vulnerability report with affected equipment manufacturer as well as:	
4.1	Law Enforcement	Additional vulnerability information (See Vulnerability Reporting Template for more information).	
4.2	Law Enforcement	Establish Responsible Disclosure period.	

Use Case	**Law Enforcement Procedures for Active Attack Use Case**		
Step	**Actor**	**Key Action**	**Comments**
4.3	Law Enforcement	Identify interim mitigation measures, if possible.	
4.4	Equipment Manufacturer	Equipment Manufacturer will push update to/contact affected state/municipal IOOs.	

Note: All identified actors have information regarding the discovered vulnerability.


Law Enforcement/Fusion Center(s)
MS-ISAC
State/Municipal CISOs
Start
Discover cybersecurity vulnerability
1
Confirm Vulnerability Report
Parallel Process
3
Inform Tier 1 (State)/Tier2 (Local) Fusion Centers
4
Inform Affected Manufacturer
2
Inform MS-ISAC (TLP:GREEN)
- Mitigation Measures
- Available patches, if any
4.1
Establish any additional vulnerability information to be included in vulnerability reports
4.2
Establish Responsible Disclosure Period
4.3
Identify Interim Mitigation Measures
Tier 1/Tier 2 Fusion Center
3.1
Verify IOOs are immediately informed
MS-ISAC
2.1 / 2.2
Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
2.1 / 3.1.1
Inform State/Municipal CISO
Each will follow their respective cyber-attack procedures, including IMP, if available.
End
End
End

Source: FHWA

Figure 11. Flowchart. UC3-S2: Law enforcement procedures for active attack use case.

Use Case 4—Security Researcher

This use case addresses when a vulnerability has been recognized by a security researcher and reports it to the equipment manufacturer.

The procedures below in Table 7 and Table 8 and information flows in Figure 12 and Figure 13 outline the flow of communication from a vulnerability discovery by a security researcher.

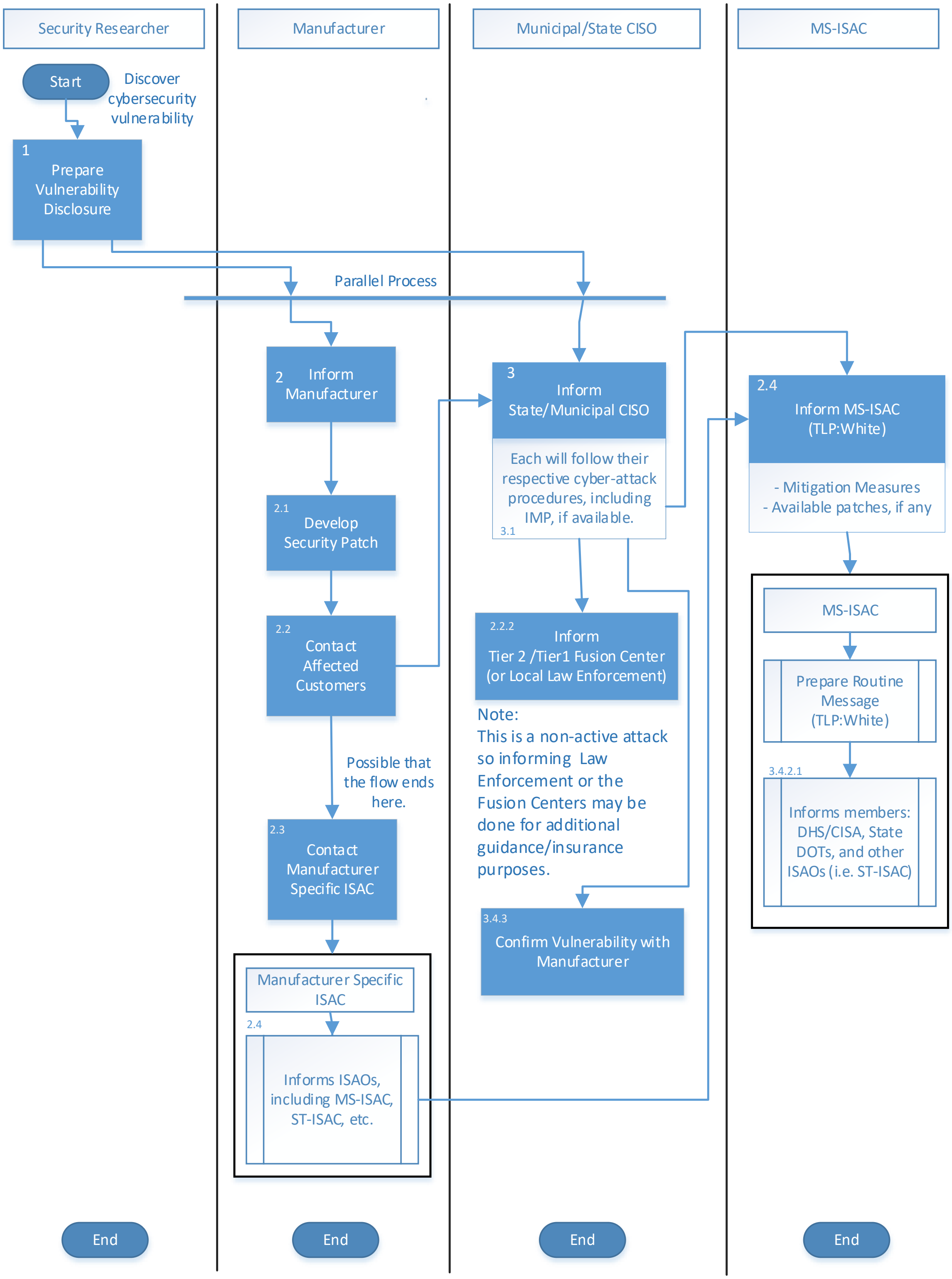
Table 7. UC4-S1: Security researcher procedures for non-active attack use case.

<table>
<tr><th>Use Case</th><th>Security Researcher Procedures for Non-Active Attack Use Case</th></tr>
<tr><td>Scenario ID & Title</td><td>UC4-S1: Security Researcher Procedures for Non-Active Attack Use Case</td></tr>
<tr><td>Scenario Objective</td><td>Make sure all the relevant stakeholders received this information reliably and quickly.</td></tr>
<tr><td>Operational Event(s)</td><td>Vulnerability has been recognized by a security researcher and reports to the equipment manufacturer. There is no indication that vulnerability is being actively exploited.</td></tr>
<tr><td>Actor(s)</td><td>
<table>
<tr><th>Actor</th><th>Role</th></tr>
<tr><td>Law Enforcement</td><td>Provides mitigation information and possible investigation if needed</td></tr>
<tr><td>DHS/CISA</td><td>Cyber Information Sharing Agency</td></tr>
<tr><td>MS-ISAC</td><td>Multi-state ISAC, large membership in transportation</td></tr>
<tr><td>State/Municipal CISO</td><td>Chief Information Security Officer, responsible for the implementation of information security policy</td></tr>
<tr><td>State/Municipal IOO</td><td>Infrastructure Owner Operators, interact with end devices</td></tr>
<tr><td>Equipment Manufacturer</td><td>Designed and developed the affected device used by IOO</td></tr>
<tr><td>Equipment Manufacturer-Specific ISAC</td><td>ISAC of which the equipment manufacturer is a member</td></tr>
</table>
</td></tr>
<tr><td>Pre-conditions</td><td>• Security researcher, following ethical practices, discovers a vulnerability and directly reports information to stakeholders.
• Details regarding cyber-attack may be missing due to gaps in equipment manufacturer/IOO information gathering.</td></tr>
</table>

Use Case	Security Researcher Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Security researcher	Security researcher will prepare vulnerability disclosure information with data points such as in Vulnerability Reporting Template.	The information in the vulnerability report will contain the previously identified data requirements to provide the minimum information needed to assist stakeholders in cyber incident information exchange.
2	Security researcher	Security researcher contacts equipment manufacturer (not contractor/reseller).	
2.1	Equipment Manufacturer	Ideally once the equipment manufacturer is informed of the issue, they will start with a security patch and continue their response by developing an update for all systems.	
2.1.1	Equipment Manufacturer	Equipment Manufacturer attempts to gather the information necessary for a vulnerability report (See Vulnerability Reporting Template for more information).	
2.2	Equipment Manufacturer	Equipment Manufacturer contacts affected customers (IOOs) with mitigation/patch	Note: Possibility that the flow ends here.
2.2.1	Municipal IOO	If the affected IOO who received assistance from the equipment manufacturer has a municipal CISO, they will share the vulnerability report with their municipal CISO.	
2.2.2	Municipal CISO	Municipal CISO may share a vulnerability report with their associated Fusion Center.	
2.3	Equipment Manufacturer	Equipment Manufacturer will share the vulnerability report with equipment manufacturer specific ISAC.	
2.4	Equipment Manufacturer-Specific ISAC	Equipment Manufacturer-specific ISAC will share the vulnerability report with the National Council of ISACs (including MS-ISAC).	

Use Case	Security Researcher Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.5	MS-ISAC	MS-ISAC will communicate vulnerability report to affected IOOs.	
2.6	MS-ISAC	MS-ISAC will prepare routine message (TLP: White broadcast) to be shared with its members.	
3	Security Researcher	If the security researcher contacts Municipal and/or State CISO:	
3.1	Municipal/ State CISOs	Each will execute their respective cyber-attack procedures, including IMP, if available.	They will coordinate as necessary with the equipment manufacturer, law enforcement, and security researcher as part of the mitigation and any criminal investigation process.
3.2	Municipal IOO	If municipal IOO has Municipal CISO.	
3.2.1	Municipal CISO	Municipal CISO reports vulnerability to State CISO/CIO.	
3.3	Municipal IOO	Else if municipal IOO does not have a Municipal CISO:	
3.3.1	Municipal IOO	Municipal IOO reports vulnerability to State CISO/CIO.	
3.4	State CISO	The following activities would then be executed by State CISO in parallel.	
3.4.1	State CISO	State CISO shares vulnerability report with other affected Municipal/State IOOs within their geographical boundaries of responsibility.	
3.4.2	State CISO	State CISO shares vulnerability report with MS-ISAC.	
3.4.2.1	MS-ISAC	MS-ISAC shares vulnerability report with equipment manufacturer's specific ISAO, DHS/CISA, and other states.	
3.4.3	State CISO	State CISO confirms vulnerability information has been shared with equipment manufacturer (not contractor/reseller).	

All identified actors have information regarding the discovered vulnerability.


Security Researcher
Manufacturer
Municipal/State CISO
MS-ISAC
Start
Discover cybersecurity vulnerability
1
Prepare Vulnerability Disclosure
Parallel Process
2 Inform Manufacturer
2.1
Develop Security Patch
2.2
Contact Affected Customers
Possible that the flow ends here.
2.3
Contact Manufacturer Specific ISAC
Manufacturer Specific ISAC
2.4
Informs ISAOs, including MS-ISAC, ST-ISAC, etc.
3
Inform State/Municipal CISO
Each will follow their respective cyber-attack procedures, including IMP, if available.
3.1
2.2.2
Inform Tier 2 /Tier1 Fusion Center (or Local Law Enforcement)
Note:
This is a non-active attack so informing Law Enforcement or the Fusion Centers may be done for additional guidance/insurance purposes.
3.4.3
Confirm Vulnerability with Manufacturer
2.4
Inform MS-ISAC (TLP:White)
- Mitigation Measures
- Available patches, if any
MS-ISAC
Prepare Routine Message (TLP:White)
3.4.2.1
Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
End
End
End
End

Source: FHWA

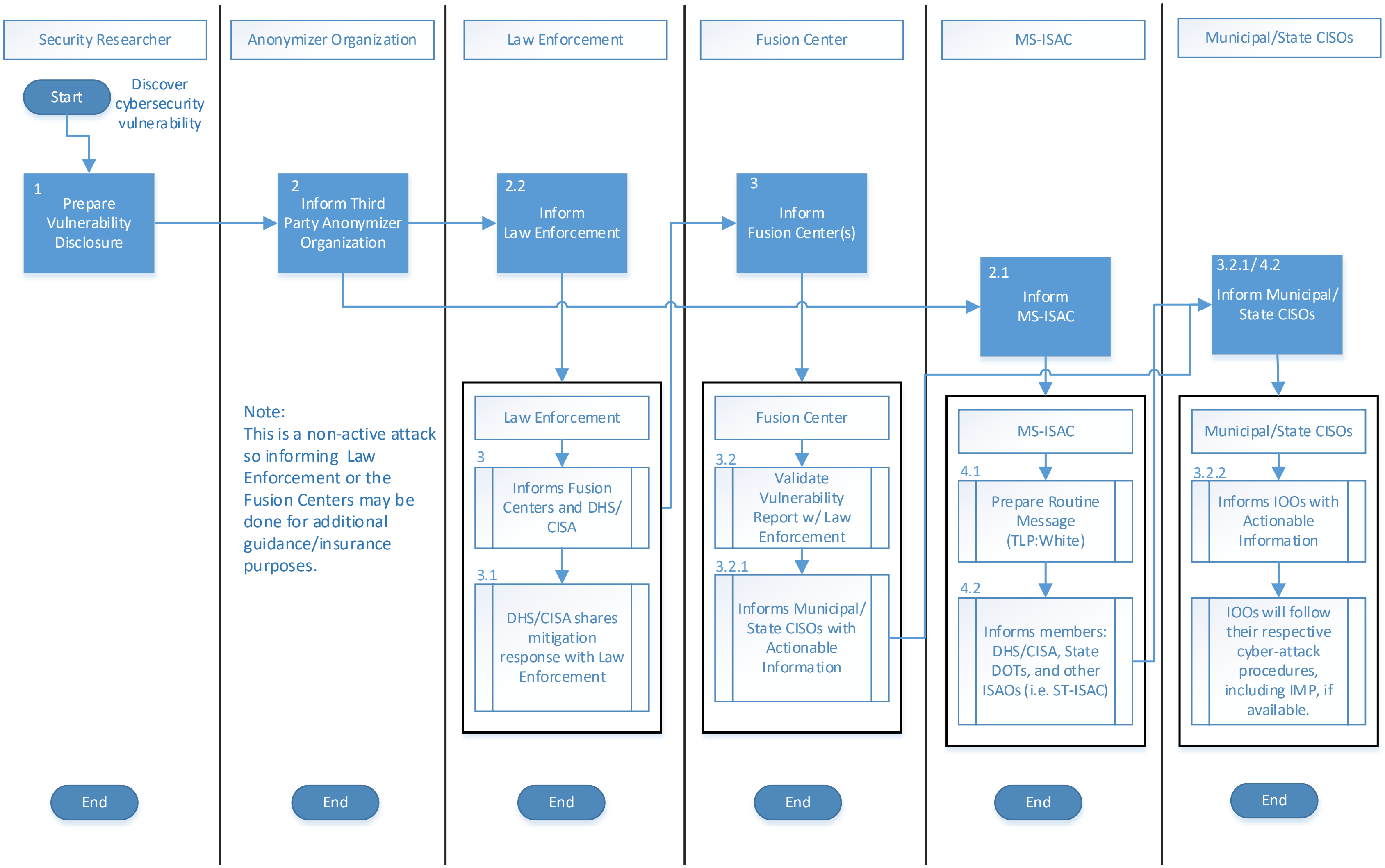
Figure 12. Flowchart. UC4-S1: Security researcher procedures for non-active attack use case.

Table 8. UC4-S2: Security researcher using anonymizer organization procedures for non-active attack use case.

Use Case	Security Researcher Using Anonymizer Organization Procedures for Non-Active Attack Use Case	
Scenario ID & Title	UC4-S2: Security Researcher Using Procedures for Non-Active Attack Use Case	
Scenario Objective	Make sure all of the relevant stakeholders received this information reliably and quickly, while protecting the identity of the security researcher that discovered the vulnerability.	
Operational Event(s)	Vulnerability has been recognized by a security researcher, who reports it to a third-party anonymizer. There is no indication that vulnerability is being actively exploited.	
Actor(s)	**Actor**	**Role**
	Law Enforcement	Provides mitigation information and possible investigation if needed
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Equipment Manufacturer	Designed and developed the affected device used by IOO
	Equipment Manufacturer-Specific ISAC	ISAC of which the equipment manufacturer is a member
	Anonymizer Organization	Third-party organization that anonymizes and then relays vulnerability information on behalf of an individual (in this case, the security researcher).
Pre-conditions	• If a security researcher discovers a vulnerability and does not want to communicate directly with stakeholders, such as the equipment manufacturer or law enforcement, they may leverage an anonymizer organization, a third-party relay organization to anonymize the notification. This anonymizer organization would then communicate to the involved parties, including the equipment manufacturers, DHS, and the IOOs. AASHTO has been considered as a potential agency for this effort but that is unconfirmed at this time. • Security researcher may or may not be acting in ethical manner when discovering the vulnerability. • Security researcher risks punishment by law enforcement. • Security researcher may or may not follow Coordinated Vulnerability Disclosure procedures or International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards 29147 Vulnerability disclosure and 30111 Vulnerability handling processes when reporting to the equipment manufacturer(s) or IOO(s).	

Use Case	Security Researcher Using Anonymizer Organization Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Security researcher	Security researcher shares vulnerability information with an anonymizer organization.	The information in the vulnerability report will contain the previously identified data requirements to provide the minimum information needed to assist stakeholders in cyber incident information exchange.
2	Third-party anonymizer	Third-party anonymizer does the following in parallel:	
2.1	Third-party anonymizer	Shares the vulnerability report with MS-ISAC.	
2.2	Third-party anonymizer	Shares the vulnerability report with Law Enforcement.	
3	Law Enforcement	Law Enforcement will share vulnerability report with Fusion Centers and DHS CISA.	
3.1	DHS/CISA	DHS/CISA shares mitigation response with Law Enforcement.	
3.2	Fusion Center	Fusion Center works with Law Enforcement to then validate the anonymous report.	
3.2.1	Fusion Center	Fusion Center creates actionable information and shares that report with State/Municipal CISOs	
3.2.2	State CISO	State CISOs share vulnerability information from Fusion Centers with affected IOOs.	IOOs will follow their respective cyber-attack procedures, including IMP, if available.
4	MS-ISAC	The following are executed in parallel following the third-party sharing information with the MS-ISAC:	
4.1	MS-ISAC	MS-ISAC will immediately communicate vulnerability advisory to affected IOOs (CVE included).	
4.2	MS-ISAC	MS-ISAC will prepare routine message (TLP: White broadcast) to be shared with its members.	

Note: All identified actors have information regarding the discovered vulnerability.


Security Researcher
Anonymizer Organization
Law Enforcement
Fusion Center
MS-ISAC
Municipal/State CISOs
Start
Discover cybersecurity vulnerability
1 Prepare Vulnerability Disclosure
2 Inform Third Party Anonymizer Organization
2.2 Inform Law Enforcement
3 Inform Fusion Center(s)
2.1 Inform MS-ISAC
3.2.1/4.2 Inform Municipal/ State CISOs
Note: This is a non-active attack so informing Law Enforcement or the Fusion Centers may be done for additional guidance/insurance purposes.
Law Enforcement
3 Informs Fusion Centers and DHS/ CISA
3.1 DHS/CISA shares mitigation response with Law Enforcement
Fusion Center
3.2 Validate Vulnerability Report w/ Law Enforcement
3.2.1 Informs Municipal/ State CISOs with Actionable Information
MS-ISAC
4.1 Prepare Routine Message (TLP:White)
4.2 Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
Municipal/State CISOs
3.2.2 Informs IOOs with Actionable Information
IOOs will follow their respective cyber-attack procedures, including IMP, if available.
End
End
End
End
End
End

Source: FHWA

Figure 13. Flowchart. UC4-S2: Security researcher using anonymizer organization procedures for non-active attack use case.

Use Case 5—Equipment Manufacturer

The following use case in Table 9 and Table 10, and information flows in Figure 14 and Figure 15 addresses when a vulnerability is reported to an equipment manufacturer concerning their product during the system verification and deployment or maintenance phases of its system development lifecycle. These use cases step through the process how manufactures notify affected IOOs.

A gap currently exists in the communication process where an equipment manufacturer does not have a clear communication path regarding vulnerabilities. To address this gap, the steps identified below are the recommended information sharing practice.

Mature equipment manufacturers establish an information sharing process that encourages proper protection of information, as well as proper disclosure while minimizing risk to their customers. An example of a mature coordinated disclosure policy for an equipment manufacturer can be found by referencing Microsoft's Coordinated Vulnerability Disclosure policy.[5] Policies like these address the disclosure of a vulnerability that affects an equipment manufacturer before it has been disclosed publicly in order to give the equipment manufacturer the opportunity to investigate and mitigate the vulnerability. Vulnerabilities may be discovered by the equipment manufacturer internally (through the typical development process, or through concentrated penetration testing), or externally via a direct contact with a security researcher (perhaps coupled with a bug bounty program).

ISO and FIRST have created standards and frameworks that pertain to the sharing and protection of information by equipment manufacturers.

- Product Security Incident Response Team (PSIRT) Services Framework (Version 1.0) https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0.pdf
- ISO/IEC 29147:2018 Information technology—Security techniques—Vulnerability disclosure https://www.iso.org/standard/72311.html
- ISO/IEC 30111:2019 Information technology—Security techniques—Vulnerability handling processes https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-2:v1:en

Equipment Manufacturers are encouraged to incorporate these standards, recommendations, and best practices.

Table 9. UC5-S1: Equipment manufacturer procedures for non-active attack use case.

Use Case	Equipment Manufacturer Procedures for Non-Active Attack Use Case
Scenario ID & Title	UC5-S1: Equipment Manufacturer Procedures for Non-Active Attack Use Case
Scenario Objective	Equipment Manufacturer discovers cybersecurity vulnerability in their product during internal cybersecurity assessment (i.e., penetration testing) and that vulnerability effects existing products deployed with clients (i.e., IOOs).

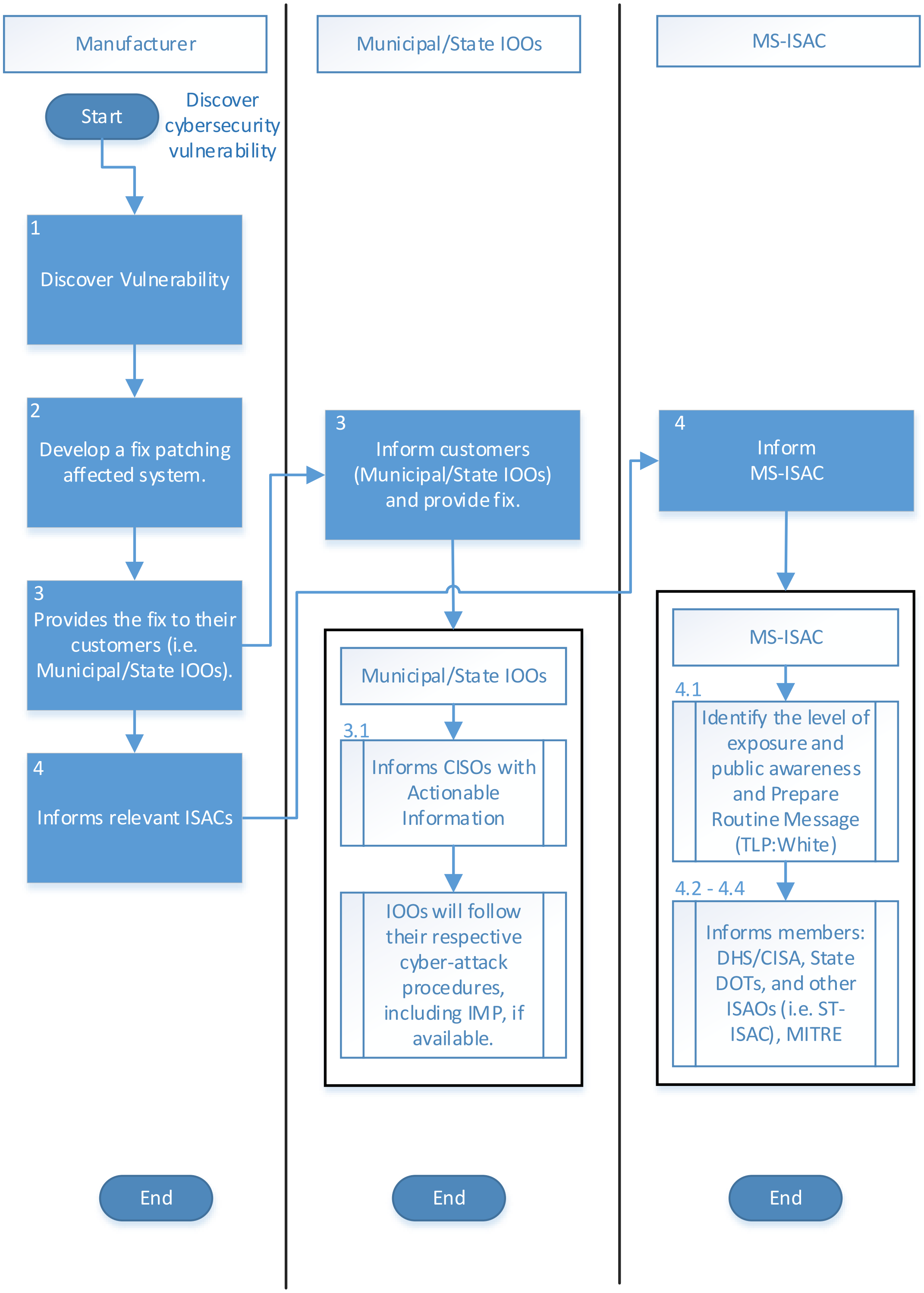
[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Alv

Use Case	Equipment Manufacturer Procedures for Non-Active Attack Use Case	
Operational Event(s)	Equipment Manufacturer provides necessary information regarding the status of a vulnerability. There is no indication that vulnerability is being actively exploited. Equipment Manufacturer provides software/firmware update.	
Actor(s)	**Actor**	**Role**
	Equipment Manufacturer	Equipment and software/firmware provider
	IOO	Equipment owner and updater
	MITRE	Agency responsible for recording and disclosure of publicly known vulnerabilities
	MS-ISAC	Agency responsible for coordination of the sharing of cybersecurity vulnerability information with IOOs and ISACs
Pre-conditions	Equipment owner uses equipment with a version of software from the equipment manufacturer with a known vulnerability	

Use Case	Equipment Manufacturer Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Equipment Manufacturer	Discover vulnerability in deployed product/production item.	
2	Equipment Manufacturer	Develop a fix patching affected system.	Fix may be in the form of a firmware/software update or hardware update.
3	Equipment Manufacturer	Provides the fix to their customers (this includes Municipal/State IOOs).	May be a tiered response with customers with the highest risk of exploitation getting priority.
3.1	Municipal/State IOOs	IOOs will follow their respective cyber-attack procedures, including IMP, if available and share vulnerability information with their CISOs.	
4	Equipment Manufacturer	Contact the MS-ISAC with a vulnerability report and identify the availability of a version without the vulnerability.	May be requested by MS-ISAC instead of broadcasted from the equipment manufacturer.
4.1	MS-ISAC	Identify the level of exposure and public awareness and create routine message with TLP identification.	

Use Case	Equipment Manufacturer Procedures for Non-Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
4.2	MS-ISAC	Create a network rule for intrusion detection equipment that can identify if the vulnerability is active.	
4.3	MS-ISAC	Communicate to IOOs if an active vulnerability is recognized.	
4.4	MS-ISAC	Communicate to MITRE if the vulnerability is publicly exposed.	MITRE may already have the information.
4.4.5	MITRE	Assign a CVE and identify the version that addresses the vulnerability	

Note: All identified actors have information regarding the discovered vulnerability


Manufacturer
Municipal/State IOOs
MS-ISAC
Start
Discover cybersecurity vulnerability
1
Discover Vulnerability
2
Develop a fix patching affected system.
3
Provides the fix to their customers (i.e. Municipal/State IOOs).
4
Informs relevant ISACs
3
Inform customers (Municipal/State IOOs) and provide fix.
Municipal/State IOOs
3.1
Informs CISOs with Actionable Information
IOOs will follow their respective cyber-attack procedures, including IMP, if available.
4
Inform MS-ISAC
MS-ISAC
4.1
Identify the level of exposure and public awareness and Prepare Routine Message (TLP:White)
4.2 - 4.4
Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC), MITRE
End
End
End

Source: FHWA

Figure 14. Flowchart. UC5-S1: Equipment manufacturer procedures for a non-active attack use case.

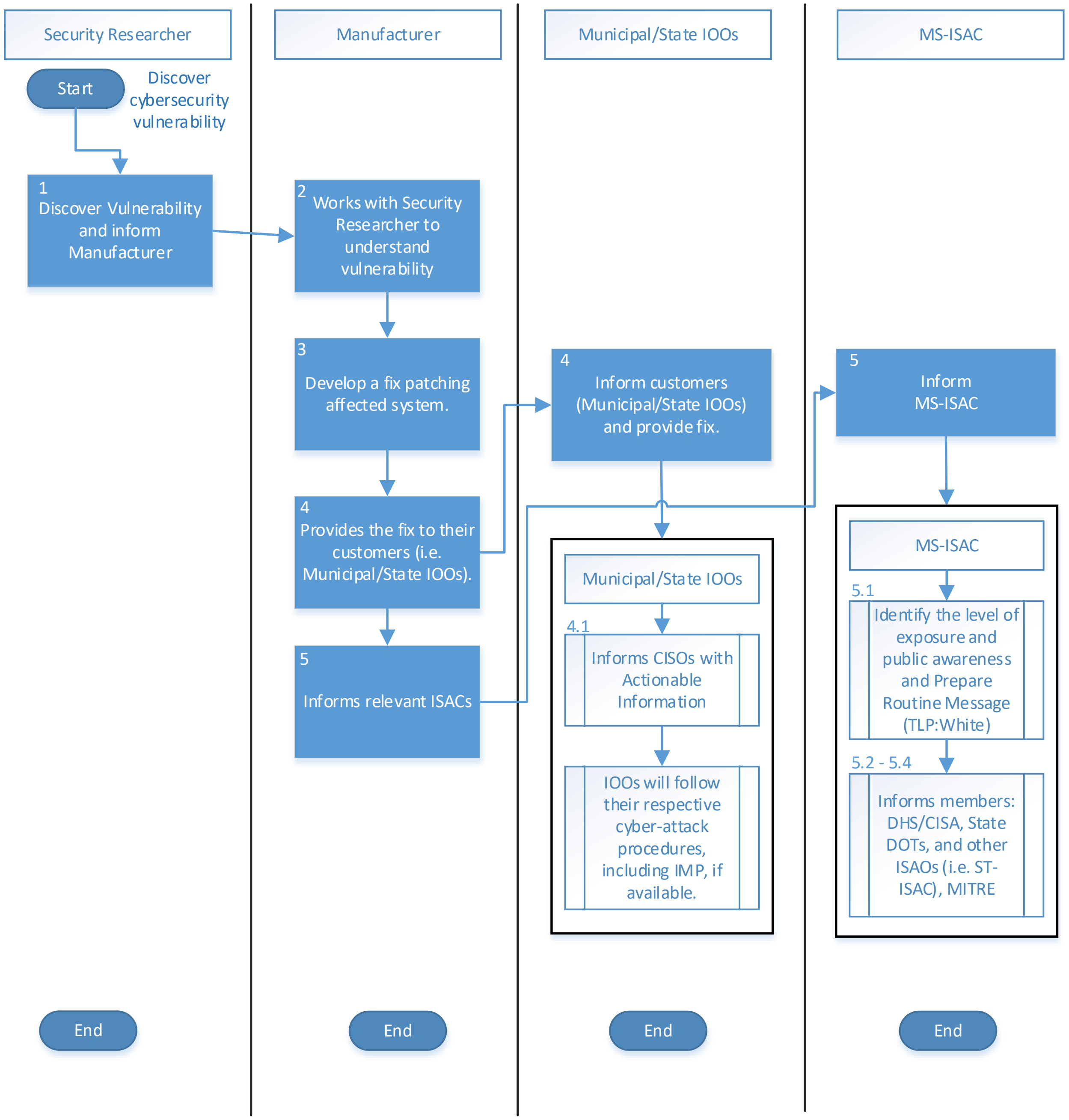
Table 10. UC5-S2: Equipment manufacturer procedures—vulnerability reported by external security researcher.

Use Case	Equipment Manufacturer Procedures—Vulnerability Reported by External Security Researcher	
Scenario ID & Title	UC5-S2: Equipment Manufacturer Learns of Vulnerability from External Security Researcher	
Scenario Objective	Equipment Manufacturer is contacted by a security researcher regarding a security vulnerability that needs to be addressed and appropriate information that needs to be shared regarding the vulnerability.	
Operational Event(s)	Security researcher provides information regarding vulnerability to the equipment manufacturer prior to public disclosure. Equipment Manufacturer provides necessary information regarding the status of a vulnerability. Equipment Manufacturer provides software/firmware update.	
Actor(s)	**Actor**	**Role**
	Security Researcher	Provide information regarding security vulnerability to Equipment Manufacturer
	Equipment Manufacturer	Equipment and software/firmware provider
	IOO	Equipment owner and updater
	MITRE	Agency responsible for recording and disclosure of publicly known vulnerabilities
	MS-ISAC	Agency responsible for coordination of the sharing of cybersecurity vulnerability information with IOOs and ISACs
Pre-conditions	Equipment owner uses equipment with a version of software/hardware from the equipment manufacturer with a known vulnerability	

Use Case	Equipment Manufacturer Procedures—Vulnerability Reported by External Security Researcher		
Step	**Actor**	**Key Action**	**Comments**
1	Security Researcher	Discover vulnerability and informs Equipment Manufacturer directly.	
2	Equipment Manufacturer	Work with security researcher to understand vulnerability.	May require discussion and have a timeline prior to publication.

Use Case	Equipment Manufacturer Procedures—Vulnerability Reported by External Security Researcher		
Step	**Actor**	**Key Action**	**Comments**
3	Equipment Manufacturer	Creates a fix for the vulnerability, patching affected system.	Steps are the same as UC5-S1 from here on:
4	Equipment Manufacturer	Provides the fix to their customers (i.e., Municipal/State IOOs).	May be a tiered response with customers with the highest risk of exploitation getting priority. IOOs will follow their respective cyber-attack procedures, including IMP, if available and share vulnerability information with their CISOs.
5	Equipment Manufacturer	Informs relevant ISACs, including the MS-ISAC with a vulnerability report and identify the availability of a version without the vulnerability.	May be requested by MS-ISAC instead of broadcasted from the equipment manufacturer.
5.1	MS-ISAC	Identify the level of exposure and public awareness.	
5.2	MS-ISAC	Create a network rule for intrusion detection equipment that can identify if the vulnerability is active.	
5.3	MS-ISAC	Communicate to IOOs if an active vulnerability is recognized.	
5.4	MS-ISAC	Communicate to MITRE if the vulnerability is publicly exposed.	MITRE may already have the information.
5.4.1	MITRE	Assign a CVE and identify the version that addresses the vulnerability.	

Note: All identified actors have information regarding the discovered vulnerability


Security Researcher
Manufacturer
Municipal/State IOOs
MS-ISAC
Start
Discover cybersecurity vulnerability
1 Discover Vulnerability and inform Manufacturer
2 Works with Security Researcher to understand vulnerability
3 Develop a fix patching affected system.
4 Provides the fix to their customers (i.e. Municipal/State IOOs).
5 Informs relevant ISACs
4 Inform customers (Municipal/State IOOs) and provide fix.
Municipal/State IOOs
4.1 Informs CISOs with Actionable Information
IOOs will follow their respective cyber-attack procedures, including IMP, if available.
5 Inform MS-ISAC
MS-ISAC
5.1 Identify the level of exposure and public awareness and Prepare Routine Message (TLP:White)
5.2 - 5.4 Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC), MITRE
End
End
End
End

Source: FHWA

Figure 15. Flowchart. UC5-S2: Equipment manufacturer procedures—vulnerability reported by external security researcher.

Use Case 6—Fusion Centers

The following use cases in Table 11 and Table 12, and information flows in Figure 16 and Figure 17 address if a Fusion Center receives a vulnerability report and how they notify affected IOOs.

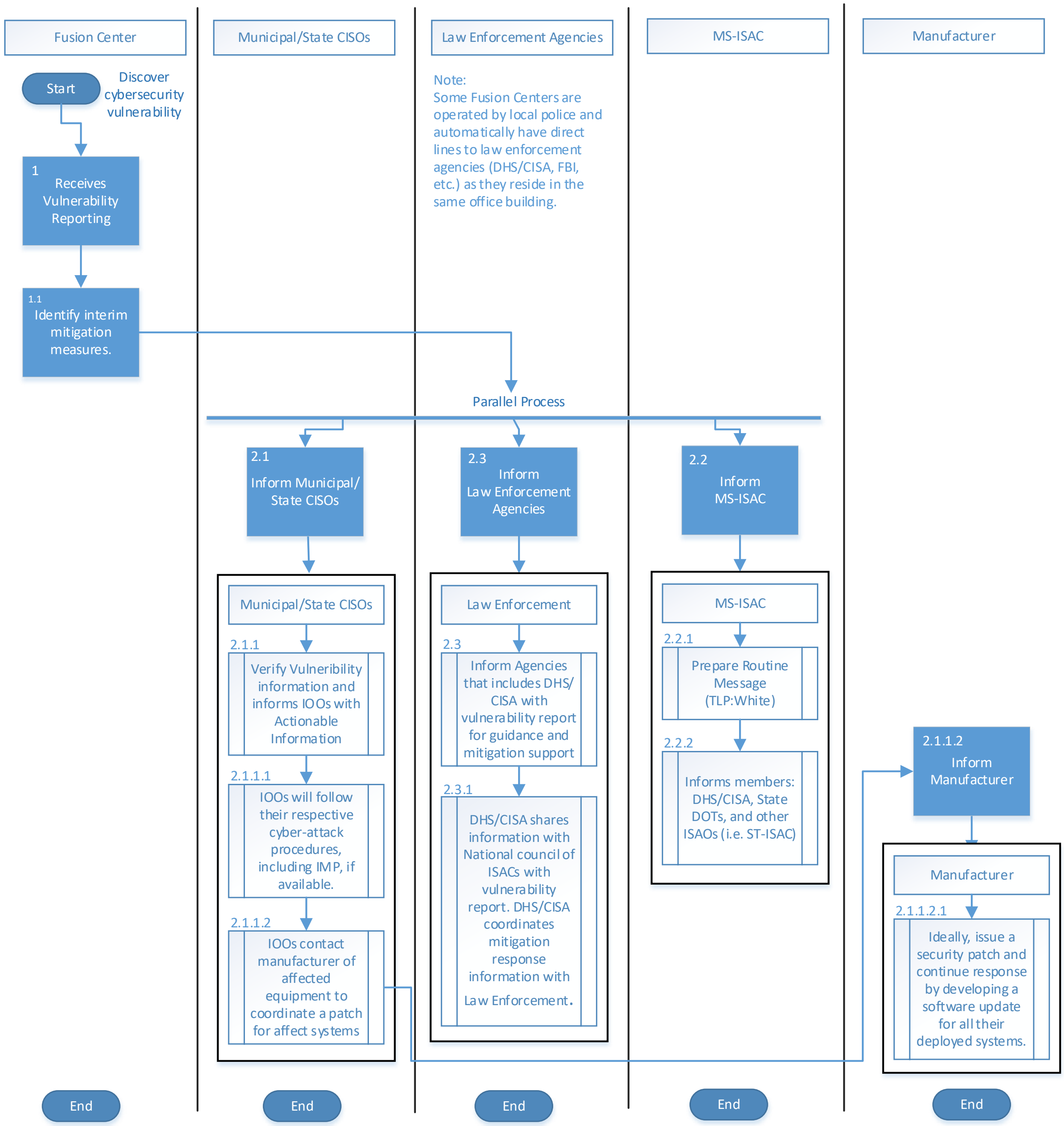
Table 11. UC6-S1: Fusion center procedures for non-active attack use case.

Use Case	Fusion Center Procedures for Non-Active Attack Use Case	
Scenario ID & Title	UC6-S1: Fusion Center Procedures for Non-Active Attack Use Case	
Scenario Objective	Detail how fusion centers notify affected IOOs	
Operational Event(s)	Receive vulnerability report in advance of active attack	
Actor(s)	**Actor**	**Role**
	Fusion Center	Receives vulnerability report
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Security Researcher	Often finds vulnerabilities, generates reports
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	Assumed that vulnerability report is generated by security researcher in advance of any active attack.	

Use Case	Equipment Manufacturer Procedures—Vulnerability Reported by External Security Researcher		
Step	**Actor**	**Key Action**	**Comments**
1	Fusion Center	Receives vulnerability reporting.	
1.1	Fusion Center	Identify interim mitigation measures.	
2	Fusion Center	Execute the following in parallel:	

Use Case	Equipment Manufacturer Procedures—Vulnerability Reported by External Security Researcher		
Step	**Actor**	**Key Action**	**Comments**
2.1	Fusion Center	Contact State/Municipal CISOs with vulnerability report.	See Vulnerability Reporting Template for more information.
2.1.1	State/Municipal IOOs	Verify vulnerability report and contact affected IOOs within areas of responsibility.	
2.1.1.1	State/Municipal IOOs	IOOs will follow their respective cyber-attack procedures, including IMP, if available, and share vulnerability information with their CISOs.	
2.1.1.2	State/Municipal IOOs	IOOs will inform equipment manufacturer of affected equipment.	
2.1.1.2.1	Equipment Manufacturer	Ideally start with a security patch and continue their response by developing a software update for all their deployed systems.	Not guaranteed to be implemented.
2.2	Fusion Center	Contact MS-ISAC with vulnerability report.	
2.2.1	MS-ISAC	Prepare routine message for distribution.	Classified as TLP:White.
2.2.2	MS-ISAC	Informs ISAC members (i.e., State DOTs) and other ISAOs (i.e., ST-ISAC) with vulnerability report from Fusion Center.	
2.3	Fusion Center	Contact Law Enforcement Agencies, including DHS/CISA with vulnerability report for guidance and mitigation support.	Some Fusion Centers are operated by local police and have law enforcement agencies (i.e., DHS/CISA, FBI), in the same office building.
2.3.1	DHS/CISA	Contact national council of ISACs with vulnerability report. DHS/CISA coordinates mitigation response information with Law Enforcement.	

Note: All identified actors have information regarding the discovered vulnerability.


Fusion Center
Municipal/State CISOs
Law Enforcement Agencies
MS-ISAC
Manufacturer
Start
Discover cybersecurity vulnerability
Note: Some Fusion Centers are operated by local police and automatically have direct lines to law enforcement agencies (DHS/CISA, FBI, etc.) as they reside in the same office building.
1 Receives Vulnerability Reporting
1.1 Identify interim mitigation measures.
Parallel Process
2.1 Inform Municipal/ State CISOs
2.3 Inform Law Enforcement Agencies
2.2 Inform MS-ISAC
Municipal/State CISOs
2.1.1 Verify Vulneribility information and informs IOOs with Actionable Information
2.1.1.1 IOOs will follow their respective cyber-attack procedures, including IMP, if available.
2.1.1.2 IOOs contact manufacturer of affected equipment to coordinate a patch for affect systems
Law Enforcement
2.3 Inform Agencies that includes DHS/ CISA with vulnerability report for guidance and mitigation support
2.3.1 DHS/CISA shares information with National council of ISACs with vulnerability report. DHS/CISA coordinates mitigation response information with Law Enforcement.
MS-ISAC
2.2.1 Prepare Routine Message (TLP:White)
2.2.2 Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
2.1.1.2 Inform Manufacturer
Manufacturer
2.1.1.2.1 Ideally, issue a security patch and continue response by developing a software update for all their deployed systems.
End
End
End
End
End

Source: FHWA

Figure 16. Flowchart. UC6-S1: Fusion center procedures for non-active attack use case.

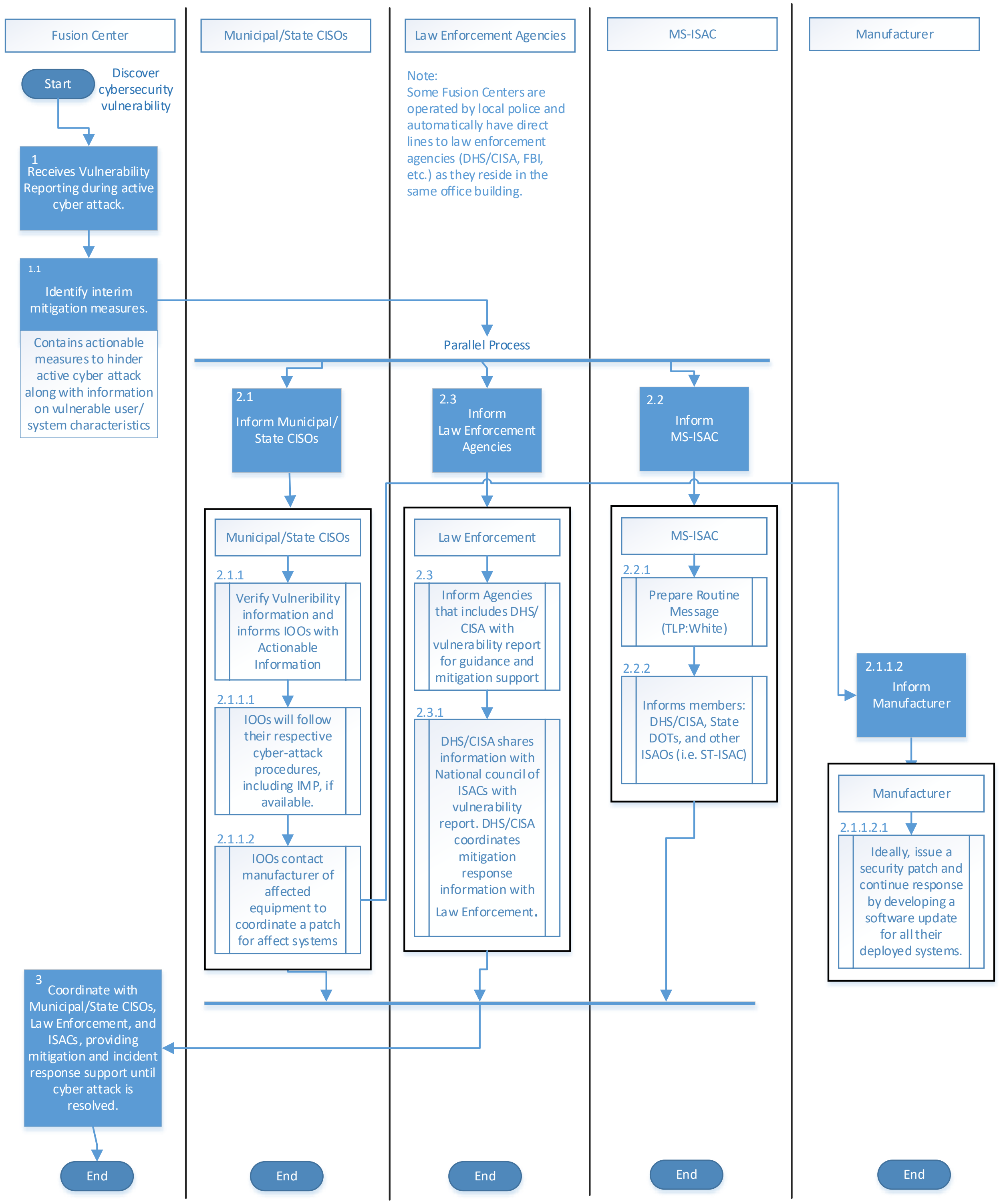
Table 12. UC6-S2: Fusion center procedures for active attack use case.

Use Case	Fusion Center Procedures for Active Attack Use Case	
Scenario ID & Title	UC6-S2: Fusion Center Procedures for Active Attack Use Case	
Scenario Objective	Detail how fusion centers notify affected IOOs.	
Operational Event(s)	Receive vulnerability reporting during active attack.	
Actor(s)	**Actor**	**Role**
	Fusion Center	Receives vulnerability report.
	DHS/CISA	Cyber Information Sharing Agency
	MS-ISAC	Multi-state ISAC, large membership in transportation
	State/Municipal CISO	Chief Information Security Officer, responsible for the implementation of information security policy
	State/Municipal IOO	Infrastructure Owner Operators, interact with end devices
	Security Researcher	Often finds vulnerabilities, generates reports
	Equipment Manufacturer	Designed and developed the affected device used by IOO
Pre-conditions	Assumed that vulnerability report is generated by affected IOO	

Use Case	Fusion Center Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
1	Fusion Center	Receives vulnerability reporting during an active cyber attack.	
1.1	Fusion Center	Identify interim mitigation measures.	Immediate mitigation information contains actionable measures to block or effect active cyber-attack. This information also contains information on vulnerable user characteristics and system characteristics.
2	Fusion Center	Execute the following in parallel:	

Use Case	Fusion Center Procedures for Active Attack Use Case		
Step	**Actor**	**Key Action**	**Comments**
2.1	Fusion Center	Contact Law Enforcement Agencies, including DHS/CISA with vulnerability report for guidance, criminal investigation support, and mitigation response support.	Some Fusion Centers are operated by local police and have Federal law enforcement agencies (i.e., DHS/CISA, FBI) in the same office building.
2.1.1	DHS/CISA	Contact national council of ISACs with vulnerability report. DHS/CISA coordinates mitigation response information with Law Enforcement.	
2.2	Fusion Center	Contact State/Municipal CISOs with vulnerability report.	See Vulnerability Reporting Template for more information.
2.2.1	State/Municipal CISOs	Verify vulnerability report and contact affected IOOs within areas of responsibility with vulnerability report and mitigation measures.	
2.2.1.1	State/Municipal IOOs	IOOs will follow their respective cyber-attack procedures, including IMP, if available, and share vulnerability information with their CISOs.	
2.2.1.2	State/Municipal IOOs	Contact equipment manufacturer of affected device to inform them regarding the vulnerability and work on a solution.	
2.2.1.2.1	Equipment Manufacturer	Ideally start with a security patch and continue their response by developing a software update for all their deployed systems.	Note: This is not guaranteed to be implemented or followed by equipment manufacturer.
2.3	Fusion Center	Contact MS-ISAC with vulnerability report and mitigation information.	
2.3.1	MS-ISAC	Prepare routine message for distribution.	Classified as TLP:White.
2.3.2	MS-ISAC	Informs ISAC members (i.e., State DOTs) and other ISAOs (i.e., ST-ISAC) with vulnerability report from Fusion Center.	
3	Fusion Center	Coordinate with Municipal/State CISOs, Law Enforcement, and ISAC, providing mitigation and incident response support until cyberattack is resolved.	

Note: All identified actors have information regarding the discovered vulnerability.


Fusion Center
Municipal/State CISOs
Law Enforcement Agencies
MS-ISAC
Manufacturer
Start
Discover cybersecurity vulnerability
Note: Some Fusion Centers are operated by local police and automatically have direct lines to law enforcement agencies (DHS/CISA, FBI, etc.) as they reside in the same office building.
1 Receives Vulnerability Reporting during active cyber attack.
1.1 Identify interim mitigation measures.
Contains actionable measures to hinder active cyber attack along with information on vulnerable user/ system characteristics
Parallel Process
2.1 Inform Municipal/ State CISOs
2.3 Inform Law Enforcement Agencies
2.2 Inform MS-ISAC
Municipal/State CISOs
2.1.1 Verify Vulneribility information and informs IOOs with Actionable Information
2.1.1.1 IOOs will follow their respective cyber-attack procedures, including IMP, if available.
2.1.1.2 IOOs contact manufacturer of affected equipment to coordinate a patch for affect systems
Law Enforcement
2.3 Inform Agencies that includes DHS/ CISA with vulnerability report for guidance and mitigation support
2.3.1 DHS/CISA shares information with National council of ISACs with vulnerability report. DHS/CISA coordinates mitigation response information with Law Enforcement.
MS-ISAC
2.2.1 Prepare Routine Message (TLP:White)
2.2.2 Informs members: DHS/CISA, State DOTs, and other ISAOs (i.e. ST-ISAC)
2.1.1.2 Inform Manufacturer
Manufacturer
2.1.1.2.1 Ideally, issue a security patch and continue response by developing a software update for all their deployed systems.
3 Coordinate with Municipal/State CISOs, Law Enforcement, and ISACs, providing mitigation and incident response support until cyber attack is resolved.
End
End
End
End
End

Source: FHWA

Figure 17. Flowchart. UC6-S2: Fusion center procedures for active attack use case.

Appendix B. Example Vulnerability Reporting Template

The following is an example of a Vulnerability Report containing the data requirements to provide the minimum information needed to assist stakeholders in cyber incident information exchange.

<u>XY-2020-03: TMC DMS Compromise at Appalachian IOO</u>

VULNERABILITY REPORT

TLP: AMBER For XY partners Only

Date of Report: March 15, 2020

Incident Severity: High

Affected Systems: TMC DMS control systems running on Windows Server Operating System with DNS services and connected IT and OT environments

<u>Threat Event Summary</u>

On March 13, 2020, a system administrator at the Appalachian IOO used his domain administrator account to check email on a Windows server, which also happened to be a DNS server Domain controller. An adversary leveraged this access to deliver a payload to the targeted DNS server. The IT network has a connection to the OT Traffic Management Center's DMS system.

The adversary was able to leverage this pathway to compromise the DMS system and modify the displays of a number of signs. The system was isolated from the IT network and signs were corrected. It was determined that the adversary had installed numerous other tools on the initially affected server. This has now been removed and rebuilt and DNS services have been moved to another server.

<u>Vulnerability Summary</u>

Researchers from Check Point identified a vulnerability in Windows DNS implementation that could allow an attacker to gain administrative access on DNS servers.

This vulnerability affects all enterprise environments that utilize the Windows DNS service.

Windows DNS servers also function as the domain controller and authority for access in the environment.

To leverage this vulnerability, the victim DNS server forwards requests to top level (root) domain servers.

For OT environments, it is best practice to separate the entire OT domain from the Internet. This includes not configuring DNS forwarders that eventually point to root DNS servers.

It is unclear if dedicated services forward these malicious requests to Microsoft DNS servers by default.

For those who have implemented a dedicated solution in place of the DNS service on domain controllers, this attack cannot be leveraged.

Vulnerability Severity: CVSS 3.x Base Score—10.0 CRITICAL

Detection and Remediation

The following sections discuss detection and remediation.

Method of Compromise

Large (>64KB) Signature (SIG) record in DNS responses can cause a buffer overflow, allowing an attacker to control allocated memory.

The vulnerability is triggered using Internet Explorer or Microsoft Edge versions that are not using Chromium, as they allow Hypertext Transfer Protocol (HTTP) requests to TCP/53.

A victim inside of the organization would have to navigate to a URL that forces a look-up to the malicious DNS server. The victim could be sent that link to make a DNS request.

Confirmation of Compromise

Monitor for unusual activity on Microsoft DNS servers.

Potential Remediation Actions

- Restrict the size of the largest inbound TCP-based DNS response via Windows Registry setting.
- Disable DNS forwarding in OT environments.
- Restrict HTTP requests over TCP/53.
- Remove DNS services from domain controllers and use a dedicated solution.

Point of Contact for Additional Information:

Bruce Wayne, Appalachian CISO

email:xxxx@xxxxx.xxx

phone:xxx-xxx-xxxx

Additional Details:

https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/cisa-releases-emergency-directive-critical-microsoft-vulnerability

https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-july-14-2020_2020-094/

https://portal.msrc.microsoft.com/en-U.S./security-guidance/advisory/CVE-2020-1350

https://nvd.nist.gov/vuln/detail/CVE-2020-1350

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350

Appendix C. Glossary of Terms

Term	Acronym	Domain	Definition	Example / Usage	Source
Access Control	-	IT	The process of granting or denying specific requests to people, devices, software, etc. in order to: 1) obtain and/or use information and related information processing services; and/or 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	Types of Access Controls include: Administrative—Defines the policies and procedures used in an organization. Physical—Devices that control access i.e., fences, gates doors, and turnstiles. See Physical Security. Logical—Access Control List Example access control scenario—User A has the role IT Administrator. User B has the role User. User A may add, remove, and modify Users, but User B may not as their role is not granted these permissions.	FIPS 201 Section C.1
Access Control List	ACL	IT	A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.	For example, login systems work on a type of access control lists. Only users maintained in the database of a system are allowed to login, thus limiting the access and actions a user can perform on the system. In an example system, users may only be able to login and access their own information, but an administrator will be able to access create/modify any users information.	NIST SP 800-179

Term	Acronym	Domain	Definition	Example / Usage	Source
Access Point	AP	IT	1) A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network. 2) An edge device that provides an entity the first point of connection to a network or network segment and should include authentication prior to assigning privilege based on user access.	A good example of an Access Point that is often interacted with is a router, switch, or Wi-Fi Access Point. These act as entry points to the enterprise network for users and will typically have some sort of security (i.e., password, device filtering) implemented.	NIST SP 800-121 Rev. 2 Appendix A, second definition derived from stakeholder feedback
Advanced Persistent Threat	APT	Cyber	AKA Advanced Persistent Threat Group. An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These groups typically utilize a recognizable attack tool and methodology, which allows them to be associated with specific attacks.	Examples of APTs include Helix Kitten, PLA Unit 61486, Cozy Bear, APT41, and APT39. APTs are responsible for the creation and release of exploits such as Stuxnet, WannaCry, EternalBlue, Gh0st RAT, and BLACKCOFFEE.	NIST SP 800-53 Rev. 4 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Advanced Traffic Management System	ATMS	Transportation	Systems that seek to reduce traffic congestion in [urban environments] by improving the efficiency of utilization of existing infrastructures.	For example, an ATMS would look at current traffic conditions, such as an accident on a freeway, and adjust surrounding traffic to prevent travel delays and further accidents. Often confused with Active Traffic Management System, which is a system with the capability to dynamically manage recurrent and non-recurrent congestion based on prevailing and predicted traffic conditions.	Advanced Traffic Management Systems: An Overview and A Development Strategy [1]
Air Gap	-	Cyber	An interface between two systems at which (a) there are no physical connections and (b) there are no automated logical connections, such as a connection to a network (i.e., data is transferred through the HMI only manually, under human control).	An example of an air gapped system is a roadside DMS that does not have remote capabilities. An operator would have to physically go to the sign to change the message displayed.	CNSSI-4009-2015 (IETF RFC 4949 Ver 2)
Asset Management (Security and Transportation)	-	Cyber	Transportation Asset Management is a strategic and systematic process of operating, maintaining, upgrading, and expanding physical assets effectively throughout their lifecycle.	Asset Management focuses on business and engineering practices for resource allocation and utilization, with the objective of better decision-making based upon quality information and well-defined objectives. For example, one part of asset management is the inventory of field devices, which includes adding, updating, maintaining, and ensuring the correction operation of devices.	FHWA, ISO 55000:2014 Sec 2.3

Term	Acronym	Domain	Definition	Example / Usage	Source
Attack	-	Cyber	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.	Often split into two distinct categories: - Active—An attack that alters data or system resources to affect their operations. This often involves some modification of the data stream or creation of falsified data. - Passive—An attack that does not alter systems or data; An attack in which the threat actor has access to data or system resources but does not try to affect them in any way. Examples of active attacks include man-in-the middle, impersonation, and session hijacking. Examples of passive attack include network traffic analysis, eavesdropping, and potentially the release of message contents.	CNSSI-4009-2015, Page 8
Attack Surface	-	Cyber	Exposed areas that make those systems more vulnerable to probes, attacks, or ability of an attacker to maintain presence in a system.	For example, an attack surface within a transportation system may be a traffic cabinet that has been left unlocked. Since this cabinet is unlocked, it leaves other systems (i.e., controller, camera controls, etc.) exposed. Within the realm of IT, things like unpatched software or falling behind on OS updates provides an "open door" like the example above.	NIST 800-53 Rev.4 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Attack Vector	-	Cyber	A segment of the entire pathway that an attacker uses to access a vulnerability.	For example, an attacker may find an open port on a workstation that does not require authentication and can further build an attack from this access point. In context, an attacker will use an Attack vector, like an open network port, in a larger attack against the system.	NIST SP 800-154 March 2016 DRAFT Section 2.1.3
Availability	-	Cyber	From the CIA triad framework: Confidentiality, Integrity, and Availability. Ensuring timely and reliable access to and use of information.	Availability in terms of a Transportation network may be the accessibility of networked field devices by the Traffic Management Center (TMC). Attackers may look to disrupt availability through the use of attacks like DoS. If no one has access to the networked field devices, then certain field operations will halt and leaving the TMC in a compromised state until the issue is mitigated.	CNSSI-4009-2015, Page 11 (44 U.S. Code Sec 3542)
Backdoor	-	Cyber	An undocumented way of gaining access to computer system.	Attackers will often create these once they have gained access to a system through use of a virus, worm, or other attack. These will often be network ports or other access methods that are not typically used by the system. These attacks may also bypass one or more access control measures.	CNSSI-4009-2015 Pg. 11 (NIST SP 800-82 Rev. 1)

Term	Acronym	Domain	Definition	Example / Usage	Source
Base station	-	IT	Remote radio equipment that governs wireless access to networks and maintains communications with client devices.	Consists of the infrastructure elements necessary to enable wireless communications, i.e., antennas, transceivers, and other electromagnetic wave transmitting equipment. Base stations are typically fixed nodes, but in a tactical environment, they may also be considered mobile.	https://www.itu.int/net/ITU-R/index.asp
Baseline Configuration	-	Cyber	A documented set of configurations for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.	An example baseline configuration is the last "working," or when all components interacted with no errors, state of the system.	NIST SP 800-53 Rev. 4 Appendix B
Blacklist	-	Cyber	A list of discrete entities (such as IP addresses, MAC addresses, URLs, process names, usernames, aliases), that have been expressly denied access based on previously determined association with malicious activity.	An example hardware blacklist would contain the MAC addresses of devices not allowed to access an organization's enterprise network due to being used in malicious ways.	NIST SP 800-94 Section 3.2.3

Term	Acronym	Domain	Definition	Example / Usage	Source
Blue Team	-	Cyber	The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically, the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).	In a mock scenario, a blue team will often defend using the security procedures and processes defined by the organization. Examples of methods that blue teams may employ include security audits, log analysis, and digital footprint analysis.	CNSSI-4009-2015, Page 13

Term	Acronym	Domain	Definition	Example / Usage	Source
Bot	-	Cyber	AKA Internet robots. AKA spiders. AKA crawlers. AKA web bots. An unmanned computer program that continuously runs a predetermined task. If malicious, then a compromised computer connected to the Internet with malicious logic to perform activities under remote the command and control of a remote administrator. When part of a larger collection of compromised computers it is known as a Botnet.	While they may be utilized to perform repetitive jobs, such as indexing a search engine, bots also come in the form of malware (see Zombie). Malware bots are used to gain total control over a computer.	CISA: National Initiative for Cybersecurity Careers and Studies (NICCS) Glossary, Section B
Botnet	-	Cyber	A large collection or string of connected bots coordinating to perform a task.	Botnets may be utilized to perform repetitive jobs, such as indexing a search engine. They often are delivered in the form of malware and are used to gain total control over a system of computers. The difference between a botnet and a bot is first the computing power available to a botnet, and second the number of computers used in a botnet (one vs. many). Typically, in a botnet, there is a command and control (C&C) node controlled by an attacker that issues commands to devices available to the botnet.	CISA: NICCS Glossary, Section B

Term	Acronym	Domain	Definition	Example / Usage	Source
Breach	-	Cyber	When sensitive, protected, or confidential information is released from a secure location to an untrusted environment by an individual unauthorized to do so.	An attacker may breach a system through the use of different attacks. This term is why organizations make use of security tools like firewalls and antivirus.	https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/Internet-fraud
Bring Your Own Device	BYOD	IT	Refers to the concept of employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.	In a TMC, this would be equivalent to an employee bringing their own device (e.g., laptop, flash drive, etc.) and connecting it to a device on the TMC network (e.g., switch, workstation, Wi-Fi.).	NIST SP 800-114 Rev.1 Section 2
Brute Force Attack	-	Cyber	An active attack that involves trying all possible combinations [of asci characters] to find a match, typically in a password.	Often, this attack is successful on passwords stored insecurely that are a short length. For example, depending on computing power available, the password "abcdefgh" would take around 5 hours maximum to brute force, but the password "abcdefghi" would take around 5 days maximum. A brute force attack requires extensive computing power and time.	NISTIR 8053 Appendix A

Term	Acronym	Domain	Definition	Example / Usage	Source
Center to Center	C2C	Transportation	A standard (see National Transportation Communications for Intelligent Transportation System Protocol [NTCIP]) dictionary defining the data format to allow traffic management centers to communicate with other centers and agencies.	An example of C2C communication is shown in two or more traffic signal systems exchanging information (including second-by-second status changes) to achieve coordinated operation of traffic signals managed by the different systems and to enable personnel at one center to monitor the status of signals operated from another center.	https://www.ntcip.org/about/
Center to Field	C2F	Transportation	A standardized (see NTCIP) communication interface between traffic management centers and devices that are deployed along roadways or other areas managed by the agency.	This communication is used by centers to communicate to field devices such as traffic signals, dynamic message signs, streetlights, and other field devices. NTCIP defines interoperability standards for each type of common field device. Examples include NTCIP 1202 for Actuated Traffic Signal Controller, NTCIP 1203 for Dynamic Message Signs. Used in this manner it is recommended to consider the use of established standards such as ITE TMDD.	https://www.ntcip.org/about/

Term	Acronym	Domain	Definition	Example / Usage	Source
Certificate Authority (CA)	-	Cyber	A trusted entity that issues and revokes public key certificates.	A certificate authority can be any server, as long as the server can be verified and trusted. Typically, a client will connect to a system, certificates will be verified on both the client and CA sides, and then encrypted communication will proceed. The most popular format for certificates is the X.509 format. Some well-known certificate authorities include Let us Encrypt, DigiCert, Symantec, and GeoTrust.	NIST SP 800-56A Rev. 3 Section 3.1
Checklist	-	Cyber	This document may also be referred to as a security configuration checklist, lockdown guide, hardening guide, security guide, security technical implementation guide (STIG), or benchmark. A document that contains instructions or procedures for configuring an IT product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized configuration changes to the product.	A checklist may include items such as: verifying IP address, verifying Domain Name System (DNS) settings, and configuring antivirus software.	NIST SP 800-70 Rev. 4 Appendix F

Term	Acronym	Domain	Definition	Example / Usage	Source
Chief Information Officer	CIO	Cyber	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.	Often, an organization will have a top-level CIO, so smaller downstream organizations (i.e., TMC) will not have a CIO. For example, TX DOT has a CIO for the entire organization who oversees the IT department, which may have offices in the different districts it oversees.	NIST SP 800-128 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Chief Information Security Officer	CISO	Cyber	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers.	Often organizations will consider their CIO to also be their CISO. Some specific goals of the CISO include: • Implementing a risk management program • Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction • Ensure the integrity, confidentiality and availability of sensitive information Some FISMA requirements include: • Maintain an inventory of information systems • Categorize information and information systems according to risk level • Maintain a system security plan • Implement security controls (NIST 800-53) • Conduct risk assessments • Certification and accreditation • Conduct continuous monitoring	NIST SP 800-128 Appendix B
Clean Word List	-	Cyber	List of words that have been pre-defined as being acceptable for transmission. Sometimes maintained by DOTs as an 'approved word list' for messages displayed on dynamic message signs.	Often used in applications like search filters. For example, if I want to search the term "Transportation Management Center," and this term has been deemed acceptable to search, the search will complete normally.	CNSSI-4009-2015, Page 19

Term	Acronym	Domain	Definition	Example / Usage	Source
Client	-	IT	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.	An example of a client is a user workstation within a Traffic Management Center (TMC).	NIST SP 800-32, pg. 47
Cloud Broker	-	IT	A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.	A specific type of Cloud Broker is a Cloud access security broker (CASBs). These are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. Examples include AWS Service Broker, IBM Cloud Brokerage Managed Services, Cloudmore, etc.	NIST SP 500-292 Appendix A
Cloud Computing	-	IT	Also referred to simply as Cloud. A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	Amazon Web Services and Azure (by Microsoft) are examples of Cloud Computing.	NIST SP 800-145 Section 2

Term	Acronym	Domain	Definition	Example / Usage	Source
Cloud Consumer	-	IT	A cloud consumer represents a person or organization that maintains a business relationship with and uses the service from a cloud provider.	A cloud consumer is anyone/anything that accesses a cloud network, e.g., a TMC workstation.	NIST SP 500-292 Appendix A
Cloud Infrastructure	-	IT	The collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.	Examples of cloud infrastructure include Amazon EC2, Google Docs, and Digital Ocean.	NIST SP 800-145 Section 2
Cloud Provider	-	IT	A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties.	Examples of providers include Amazon, Oracle, and Google.	NIST SP 500-292 Appendix A

Term	Acronym	Domain	Definition	Example / Usage	Source
Commercial off-the-shelf	COTS	IT	Also referred to as off-the-shelf. Software and hardware that already exists and is available from commercial sources.	An example of widely used COTS software are Microsoft Office products.	NIST SP 800-161 Appendix F
Common Vulnerabilities and Exposures	CVE	Cyber	A nomenclature and dictionary of security-related software flaws.	For example: CVE-2020-1720 describes a flaw discovered in a particular SQL implementation.	CNSSI-4009-2015, Page 22
Common Vulnerability Scoring System	CVSS	Cyber	An open framework for communicating the characteristics and severity of software vulnerabilities.	CVSS is a scoring system used during security assessments to enable a common understanding of vulnerability severity. It allows organizations, equipment manufacturers/vendors, and security researchers to have common point for interpreting what a high, medium, or low risk severity means for a particular asset or item and connected environment. For example, a MySQL Stored SQL Injection (CVE-2013-0375) is scored at a 6.4 (on a scale between 0 and 10, where 10 is an extremely harmful and easy to deploy vulnerability) using CVSS v.3.1. More examples of CVSS scoring can be found at: https://www.first.org/cvss/examples	https://nvd.nist.gov/vuln-metrics/cvss

Term	Acronym	Domain	Definition	Example / Usage	Source
Compromise	-	Cyber	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.	An example compromise is unauthorized access (i.e., breach) to user data.	CNSSI-4009-2015, Page 24
Computer Incident Response Team (CIRT)	-	Cyber	Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Computer Incident Response Team (CIRT) is also known as Computer Security Incident Response Team (CSIRT), CIRC (Computer Incident Response Center, Computer Incident Response Capability, and Cyber Incident Response Team).	An example of a CIRT mission statement, or way that they operate, may be: “It is the mission of XYZ CIRT to protect XYZ by creating and maintaining the capability of detecting, responding and resolving computer and information security incidents.” In response to an incident, the CIRT may perform actions like forensics, network log analysis, and file system analysis to determine what transpired during an attack so that they can implement changes to fix it.	NIST SP 800-137 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Concept of Operations	ConOps	Transportation	A description of how a system will be used. It is non-technical and presented from the viewpoints of the various stakeholders. This provides a bridge between the often-vague needs that motivated the project to begin with and the specific technical requirements.	The ConOps is designed to give an overall picture of the organization operations. It provides the basis for bounding the operating space, system capabilities, interfaces, and operating environment. In general, it will include the following: • Statement of the goals and objectives of the system • Strategies, tactics, policies, and constraints affecting the system • Organizations, activities, and interactions among participants and stakeholders • Clear statement of responsibilities and authorities delegated • Specific operational processes for fielding the system • Processes for initiating, developing, maintaining, and retiring the system It is important that an organization has a ConOps in place for contingency and everyday operations.	https://www.fhwa.dot.gov/cadiv/segb/views/document/sections/section8/8_4_5.cfm

Term	Acronym	Domain	Definition	Example / Usage	Source
Confidentiality	-	Cyber	From the CIA triad framework: Confidentiality, Integrity, and Availability. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them.	Confidentiality considers the privacy of any information that a business or individual does not want to be public and minimizing the information's usage and secure storage. For example, efforts to preserve release of personally identifiable information only to authorized individuals falls under confidentiality.	CNSSI-4009-2015 Pg. 30
Conflict Monitor	-	Transportation	Also known as Malfunction Management Unit (MMU). A device configured to check for conflicting signal indications and various other malfunctions including absence of an OK status output from the controller (watchdog output), short or missing clearance intervals, and out-of-range operating voltages.	The conflict monitor prevents unsafe conditions at an intersection, such as all green lights. If an unsafe condition is detected, the conflict monitor overrides the system and switches to flashing red lights.	https://ops.fhwa.dot.gov/publications/fhwahop06006/chapter_7.htm
Contingency Plan	-	Cyber	A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.	An example contingency plan is to restore all devices to a baseline configuration. In the case of an emergency or cyber event, this would prevent devices from being unavailable and ensure normal operations.	NIST SP 800-57 Part 1 Rev. 4 Section 2

Term	Acronym	Domain	Definition	Example / Usage	Source
Continuity of Operations Plan	COOP	IT	An organized procedure to allow a business or organization to function through an interruption.	COOP is used to restore an organization's mission essential functions (MEF) at an alternate site and performing those functions while normal operations are restored.	NIST SP 800-34 Rev. 1 Appendix G
Continuous Monitoring	-	Cyber	Maintaining ongoing awareness to support organizational risk decisions.	Continuous monitoring may include network analysis and vulnerability scanning. For example, organizations may use software that monitors devices connected to their networks for malware or vulnerabilities on those devices to better their network's security.	NIST SP 800-137 Chapter 1
Credential	-	Cyber	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a card or token possessed and controlled by a cardholder or subscriber.	A credential may be physical or digital, with the simplest example being a username and password that are used to identify a user for accessing a website.	NIST SP 800-79-2 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Critical Infrastructure	-	Cyber	System and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	A major piece of critical infrastructure used every day at a TMC is the TMS. Without the control of traffic operations, national public safety would be compromised. Another example at the field level would be traffic signals. Without the use of these signals, public health is at risk due to the increased likelihood of traffic accidents. Sectors include Information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping (NIST SP 800-30 Rev. 1).	CNSSI-4009-2015 Pg. 34
Cryptography		Cyber	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.	In order to secure data in transit or at rest, cryptographic algorithms (with acronyms such as RSA, AES, DES) would be used to protect the data from inappropriate use. Cryptographic methods are used in a wide variety of applications to secure data including: Asymmetric Key Cryptography Elliptic Curve Cryptography Public Key Cryptography Asymmetric Key Cryptography Private Key Cryptography Symmetric Key Cryptography	CNSSI-4009-2015 Pg. 39

Term	Acronym	Domain	Definition	Example / Usage	Source
Cyber Hygiene	-	Cyber	Addresses the simple sets of actions that users can take to help reduce cybersecurity risks.	Good cyber hygiene includes practices such as: • User authentication before accessing a system • Good password practices (10-char password, letters, numbers, special characters, etc.) • Use of antivirus and firewalls • Maintaining a cyber-aware team • Constant monitoring of networks and devices on networks It is important to maintain a good cyber hygiene, as this will prevent attacks and data leakage.	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540924
Cyber Security	-	Cyber	Also referred to as simply as Cyber or as one word “cybersecurity.” The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.	Cyber security is the top level for most of the terms listed in this document, and thus there are many examples.	https://www.us-cert.gov/ncas/tips/ST04-001

Term	Acronym	Domain	Definition	Example / Usage	Source
Cyber Threat Actor	CTA	Cyber	AKA Threat Actor. AKA Threat Agent. An individual, group, organization, or Government that conducts or has the intent to conduct detrimental activities. Participant (person or group) in an action or process that is characterized by malice or hostile action (intending harm) using computers, devices, systems, or networks.	CTAs are classified into one of five groups based on their motivations and affiliations: Cybercriminals, Insiders, Nation-State, Hacktivists, Terrorists Organizations A specific example of a group of CTAs include the hacker group Anonymous.	CISA: NICCS Glossary, Section T
Cyber Threat Actor—Level 1	CTA-1	Cyber	The lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Motivated often by curiosity about how things work. Could be non-malicious and disruption are sometimes inadvertent.	Examples of these types of CTAS include Script Kiddies.	https://ics-cert-training.inl.gov/learn/course/external/view/elearning/50/210W-06ICSCybersecurityThreats
Cyber Threat Actor—Level 2	CTA-2	Cyber	Generally understood to have less sophistication in comparison to level 3, more experienced and have greater capabilities than level 1. Motivated often by desire to disrupt operations, retaliation, or financial gain.	Examples of these types of CTAS include Insider threat, cyber criminals / malicious hackers, Hacktivists	https://ics-cert-training.inl.gov/learn/course/external/view/elearning/50/210W-06ICSCybersecurityThreats

Term	Acronym	Domain	Definition	Example / Usage	Source
Cyber Threat Actor—Level 3	CTA-3	Cyber	The most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination. Capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their strategic goals, which may include bringing down critical operations or causing maximum damage to infrastructure/public.	Examples of these types of CTAS include Nation-state, Terrorist Organizations, APTs.	https://ics-cert-training.inl.gov/learn/course/external/view/elearning/50/210W-06ICSCybersecurityThreats
Data Diode	-	IT	A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction.	Often, a data diode will be used at the edge of a network, for example allowing a workstation to reach out to a field device but not allowing any network traffic to reach back.	NIST SP 800-82 Rev. 2 Appendix E
Data Integrity	-	Cyber	The property that data is complete, intact, trusted, and has not been altered in an unauthorized or accidental manner. Data integrity covers data in storage, during processing, and while in transit.	Data integrity is essential in the operation and security of agencies and businesses and is the primary goal digital signatures. Measures to ensure Data Integrity look to ensure what was originally transmitted is identical to what is received and to prevent attacks like Data Leakage or Breaches.	CNSSI-4009-2015 Pg. 41

Term	Acronym	Domain	Definition	Example / Usage	Source
Data Loss Prevention	DLP	Cyber	A set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.	Often used to prevent Data Leakage. Tools used in data loss prevention include: firewalls, intrusion detection systems (IDSs) antivirus software, machine learning and temporal reasoning algorithms to detect abnormal access to data, and systems that detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, mainly by personnel who are authorized to access the sensitive information. Data Loss Prevention and its associated tools/methods are used by organizations to limit Risk and potential Attacks.	Liu, S., & Kuhn, R. (2010, March/April). Data loss prevention. IEEE IT Professional, 11(2), pp. 10-13.
Decryption	-	Cyber	The process of converting encrypted data back into its original form, so it can be understood. Related term: Encryption.	Once a communication package has been received, the receiving device decodes the data (decryption) so that it can be used by the device. One traffic management center encrypts data before sending it to another traffic management center. This prevents the data from being received and interpreted by a third listening party. The receiving traffic management center decrypts the data in order to be used.	CISA: NICCS Glossary, Section D

Term	Acronym	Domain	Definition	Example / Usage	Source
Defense in Depth	-	Cyber	The principle of implementing layered security (ensure no single point of vulnerability). Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability.	For example, the IT group in a TMC may have firewalls and antivirus in place, but this does not always protect users from malicious emails and web applications. To avoid this, defense-in-depth will suggest continuous monitoring of network traffic to catch if the firewall fails.	NIST 800-53 Rev.4 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Demilitarized Zone	DMZ	IT	In computer security, a DMZ or perimeter network is a network area (a subnetwork) that sits between an internal network and an external network. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network—hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end. The Security DMZ is used for providing external controlled access to services used by external personnel to the control system network control system equipment to ensure secure application of system updates and upgrades.	The Security DMZ is used for providing external controlled access to services used by external personnel to the control system network control system equipment to ensure secure application of system updates and upgrades. e.g., a user inside a firewall needs to publish information to the outside.	CISA: Control System Security DMZ Definition

Term	Acronym	Domain	Definition	Example / Usage	Source
Denial of Service Attack	DoS	Cyber	An attack that makes legitimate users unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Related term: active attack.	An example DoS attack would be flooding a network with traffic such that others could not access the network.	https://www.us-cert.gov/ncas/tips/ST04-015
Detect	-	Cyber	Part of the NIST cybersecurity framework core functions. Appropriate activities to recognize the occurrence of a cybersecurity incident. Also enables timely recognition of cybersecurity incidents.	This term is often tied to intrusion or attack detection. Methods of detection include timing-based approaches, port monitoring, and profile monitoring. Detection of attacks is important as lack of this capability leaves organizations at risk for greater compromise of their systems.	NIST Cyber Framework
Dirty Word List	-	Cyber	List of words that have been pre-defined as being unacceptable for use within an application or system. May be used in conjunction with a clean word list to avoid false negatives (e.g., secret within secretary).	Often used in applications like search filters or for equipment such as DMS. Words on the Dirty Word List would be prevented from being used and could be flagged by the system. A common attack on DMS is to post "Zombies Ahead" and the word "Zombies" could be included in the Dirty Word List to recognize when an unauthorized user was trying to modify the sign's message.	CNSSI-4009-2015 Pg. 45

Term	Acronym	Domain	Definition	Example / Usage	Source
Distributed Denial of Service (DDOS)	-	Cyber	A denial-of-service technique that uses numerous hosts to perform the attack.	This attack method is used when the bandwidth needed to deny service (i.e., overload a communication channel) exceeds that available to only one computer. Those devices can then be used to perform coordinated denial of service attacks from all of the devices, targeting one specific target or network. This is sometimes called a botnet.	CNSSI-4009-2015 Pg. 46
Domain Name System	DNS	IT	System that translates domain (e.g., www.google.com) names to IP addresses and back.	For example, IT policy may allow a computer to reference both a primary and secondary DNS, one for external connections and internal connections. This could lead to an attacker sending a user to an unintended malicious site through falsified DNS resolutions.	NIST SP 800-81-2
Dynamic Messaging Sign	DMS	Transportation	AKA changeable message sign (CMS). AKA Variable Message Sign (VMS). Any transportation sign system that can change the message presented to the viewer. It includes the following major components: sign face, sign housing, controller, and, if present, the controller cabinet.	See Appendix D for an example.	https://www.ntcip.org/wp-content/uploads/2018/11/NTCIP1203v03f.pdf, section 1.4
Egress	-	IT	Network communication that originates inside of one network and is provided to a destination outside of that network.	A command sent from a server inside the traffic management center to a field device through the center's firewall is an example of egress.	NIST SP 800-41 Rev. 1 Appendix A

Term	Acronym	Domain	Definition	Example / Usage	Source
Encryption	-	Cyber	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. When used as a verb, the term is "encrypt" or to reverse the transformation, the term is "decrypt.” Related terms: decryption, cryptography.	See example of encrypting the word “Hello” using an encryption algorithm known as ROT13 in Appendix D.	NIST SP 800-82 Rev. 2 Appendix E
End-to-end encryption	-	Cyber	Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.	End-to-end encryption protects the data from being decoded while being transferred and is the foundation for network security.	NIST SP 800-12 Rev. 1 Appendix B
Exploit	-	Cyber	The means through which a vulnerability can be leveraged for malicious activity by hackers.	Known exploits are tracked by MITRE using a standardized naming strategy as Common Vulnerabilities and Exposures (CVE). An example of a well-known exploit would be CVE-2015-5611 which was leveraged in the Jeep hack in 2015 to remotely control the functionality of a Jeep Grand Cherokee.	https://www.ncsc.gov.uk/information/how-cyber-attacks-work

Term	Acronym	Domain	Definition	Example / Usage	Source
Exploit Kit	-	Cyber	Toolkits that automate the exploitation of vulnerabilities in popular software applications in order to maximize successful infections and serve as a platform to deliver malicious payloads such as Trojans, spyware, bit coin mining software, ransomware, and other malicious software.	The adobe flash player and Microsoft Explorer are common targets of exploit kits, due to known vulnerabilities and common usage of these products. Examples of exploit kits includes MPack, Metasploit, Phoenix, and others. Exploit kits are frequently used by CTA-1 and CTA-2s reusing exploits created by other attackers. Use of exploit kits allow an attacker to exploit vulnerabilities normally beyond their technical capabilities. This increases the risk to systems with vulnerabilities covered by an exploit kit.	NJ Cybersecurity & Communications Integration Cell (NJCCIC): Exploit Kits
Fault Tolerant	-	IT	Of a system, having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.	A method often used in fault tolerance is system backup. If there is a restorable version after the detection of a fault/error, availability of the system can be restored.	NIST SP 800-82 Rev. 2 Appendix B
Federated Understanding of Security Information Over Networks	FUSION	Cyber	Process that works with each Federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats.	See a description of FUSION on Digital Operatives website. If a user is unsure of the reason for compromise, or that a compromise has even occurred, they may refer to the FUSION platform for assistance in understanding the compromise.	CISA

Term	Acronym	Domain	Definition	Example / Usage	Source
Field Device	-	Transportation	Also known as edge device, roadside equipment. Equipment that is connected to the field side on an Industrial Control System (ICS). Related terms: changeable message sign, traffic signal controller.	Types of field devices include traffic controllers, cameras, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) devices, actuators, sensors, and associated communications.	NIST SP 800-82 Rev. 2 Appendix B
Firewall	-	IT	An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be “inside” the firewall) and thus protects that network’s system resources against threats from the other network (the one that is said to be “outside” the firewall).	An example firewall is an access point configured with software to provide blacklisting, IP address filtering, or MAC address filtering capabilities.	NIST SP 800-82 Rev. 2 Appendix B
Firmware	-	Transportation	Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that the programs and data cannot be dynamically written or modified during execution of the programs	Examples of firmware includes code that controls printers or digital clocks. Older traffic signal controller will still run program from firmware, whereas a newer traffic signal controller may not use firmware to run programs.	CNSSI-4009-2015, page 54

Term	Acronym	Domain	Definition	Example / Usage	Source
Forensics	-	Cyber	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.	A forensic investigation may be performed after an intrusion has been discovered, where all computer evidence and network logs are analyzed by investigators in order to learn the method of attack, identify any traces of the attackers and address the problem or communicate the concern to other agencies. Forensics are typically used for criminal or civil legal proceedings.	CNSSI-4009-2015, Page 55

Term	Acronym	Domain	Definition	Example / Usage	Source
Fusion Center	-	Cyber	Fusion Centers are organizations that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), Federal and private sector partners	State fusion centers such as the Florida Fusion Center or regional fusion center such as the Boston Regional Intelligence Center are responsible for managing the flow of information across Government agencies and the private industry. Often split between: • Primary—Provides information sharing and analysis for an entire state. These centers are the highest priority for the allocation of available Federal resources, including the deployment of personnel and connectivity with Federal data systems. • Recognized—A recognized fusion center typically provides information sharing and analysis for a major urban area. As the Federal Government respects the authority of state governments to designate fusion centers, any designated fusion center not designated as a primary fusion center is referred to as a recognized fusion center.	DHS: Fusion Centers
Gateway	-	IT	A device on a network that serves as an entrance to another network.	See example for firewall. These devices will often filter access to networks by IP address, MAC address, or other criteria.	ISACA Glossary, Section G

Term	Acronym	Domain	Definition	Example / Usage	Source
Global System for Mobile Communications	GSM	IT	A set of standards for second generation cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP). These standards handle voice efficiently but provides limited support for data and Internet applications.	Various spectrums for GSM are used in different parts of the world, with GSM 900 / GSM 1800 MHz used in most parts of the world (Europe, Asia, Australia, Middle East, Africa) while GSM 850 / GSM 1900 MHz are used in the United States, Canada, and Mexico.	https://www.itu.int/osg/spu/ni/3G/casestudies/GSM-FINAL.pdf
Hacker	-	Cyber	Unauthorized user who attempts to or gains access to an information system.	While typically viewed from a negative connotation, hacker is a broad category of that can be broken out into smaller categories depending on the motivations, specific actions, or intent of the individual. Hackers take many roles; from those who are looking to cause damage or steal information, to those who seek to expose issues to raise awareness and safety. Identifying a hacker is unusual, though some of the more prominent hackers include Kevin Mitnick, Charles Miller, and Chris Valasek.	NIST SP 800-12 Rev. 1 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Honeypot	-	Cyber	A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential hackers and intruders. Often, this system includes only fake or random data without true value. The name is a reference to the attraction of honey to bears, with the possibility of getting the bear stuck in the honey pot.	For example, an IT department may put a honeypot on the same network as a gateway to the internal network to prevent attackers from attempting to attack the gateway and gain further network access.	CNSSI-4009-2015, Page 58
Human Machine Interface	HMI	IT	The hardware or software through which an operator interacts with a controller.	An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. Often is the form of a Microsoft Windows GUI.	NIST SP 800-82 Rev. 2 Appendix B
Hypertext Transfer Protocol	HTTP	IT	An application-layer protocol for transmitting hypermedia documents.	HTTP is the underlying protocol used in most all web-based communication.	https://tools.ietf.org/html/rfc1945
Hypertext Transfer Protocol Secure	HTTPS	IT	Hypertext Transfer Protocol transmitted over Transport Layer Security.	Though this is used on most websites, HTTPS is especially important when Personally Identifiable Information (PII) or other sensitive information is being transmitted over the web (e.g., financial data, credit card transactions, and social security numbers).	https://tools.ietf.org/html/rfc2818

Term	Acronym	Domain	Definition	Example / Usage	Source
Identify	-	Cyber	Part of the NIST cybersecurity framework core functions. Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. In the context of a cyber incident, establish or indicate the scope of a security vulnerability, often including a name.	In the context of investigating a cyber incident or discovering a vulnerability, the threat must first be identified, typically including the assets that are affected and what is the extent of the vulnerability.	NIST Framework V1.1, Section 2.1
Impact Analysis	-	Cyber	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events, such as data breaches or attackers attempting to hack and organization.	Impact analysis may include use of CVSS or other scoring methods in combination with risk analysis and assessment to determine a particular component impact if affected. For example, the CVSS score for the OpenSSL Heartbleed vulnerability is 7.5, but the breakout for this score states that there is a high impact to confidentiality. When performing an impact analysis, if the organization is often transmitting sensitive data, this vulnerability would be considered highly damaging and should be protected against.	ISACA Glossary, Section I

Term	Acronym	Domain	Definition	Example / Usage	Source
Incident	-	Cyber	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. This can be due to an active attack that interrupts normal operation, or due to malfunction or misuse of information system components.	An example of an incident may be DoS attack or a user accessing unauthorized information.	NIST SP 800-61 r2, Appendix C
Incident Response	-	Cyber	The mitigation of violations of security policies and recommended practices.	An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.	NIST SP 800-61 r2, Appendix C

Term	Acronym	Domain	Definition	Example / Usage	Source
Industrial Control Systems Cyber Emergency Response Team	ICS-CERT	IT	Team that provides a control system security focus in collaboration with U.S.-CERT to: • Conduct vulnerability and malware analysis • Provide onsite support for incident response and forensic analysis • Provide situational awareness in the form of actionable intelligence • Coordinate the responsible disclosure of vulnerabilities/mitigations • Share and coordinate vulnerability information and threat analysis through information products and alerts.	For example, if a vulnerability discovered by U.S.-CERT was found to affect ICS devices, the ICS-CERT would then provide s	https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf

Term	Acronym	Domain	Definition	Example / Usage	Source
Industrial Control System	ICS	IT	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy.	Industrial control systems are used to monitor and command processes at power plants, transportation industries, and other critical infrastructure. Industrial control systems may make use of supervisory control and data acquisition (SCADA) systems which are used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers (PLCs) to control localized processes.	NIST SP 800-82 r2, Appendix B
Industrial Internet of Things	IIoT	IT	IoT with a focus on industrial devices. IoT and IIoT Ecosystems may utilize similar sensors but the service provider performs different tasks.	For example, controlling the function of a traffic-restricting gate from a remote location using IIoT sensors. This is contrasted with smart home devices, a typical use case of IoT, which are typically used by a homeowner to control aspects of their home (e.g., door locks, air conditioning).	https://www.us-cert.gov/sites/default/files/2019-07/Understanding_of_IoT_and_IIoT_Ecosystems_S508C.pdf

Term	Acronym	Domain	Definition	Example / Usage	Source
Information Security Testing	-	Cyber	The process of validating the effective implementation of security controls for information systems and networks, based on the organization’s security requirements.	Examples of a security test may include testing an IT or field device network for vulnerabilities.	NIST SP 800-115, Appendix F
Information Sharing and Analysis Center	ISAC	Cyber	Member-driven organizations that deliver all-hazards threat and mitigation information to asset owners and operators. Many of them also support incident response and recovery activities.	Center for Internet Security (CIS) operates both the MS-ISAC® and the Elections Infrastructure ISAC®, to provide a variety of services, including monitoring by a 24/7 SOC. The MS-ISAC collects, analyzes, and disseminates cyber threat information regarding the presentation, protection, response, and recovery to their members consisting of U.S. State, Local, Tribal, and Territorial (SLTT) governments. Disclosure of information is internal and restricted to members except by preset rules or individual consent.	National ISAC Site

Term	Acronym	Domain	Definition	Example / Usage	Source
Information Technology	IT	IT	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. IT supports business-oriented applications and often utilizes high-capacity computing power. Contrast to OT.	The term IT includes examples such as personal computers or commercial servers along with the network equipment to connect this equipment together. The IT domain works with computing equipment that can serve multiple purposes. This contrasts with OT, where the computing equipment capabilities are limited to the exact functionality that is required.	NIST SP 800-128 Appendix B
Insider	-	Cyber	Any person with authorized access to any organization resource which includes personnel, facilities, information, equipment, networks, or systems.	This includes all employees within an organization and highlights the need for an insider threat program.	CNSSI-4009-2015 pg. 67
Insider Threat	-	Cyber	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of an organization.	An example of an insider threat is Chelsea Manning, who used her position to steal documents from the U.S. Military and send them to media outlets.	CNSSI-4009-2015 pg. 67

Term	Acronym	Domain	Definition	Example / Usage	Source
Integrity	-	Cyber	From the CIA triad framework: Confidentiality, Integrity, Availability Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	Integrity is essential in the operation and security of agencies and businesses. It is guaranteed using security tools, like hashing, such that what was originally transmitted can be checked and verified as being identical to what is received.	CNSSI-4009-2015, Page 68 [44 U.S.C. Sec. 3542]
Intelligent Transportation System	ITS	Transportation	A system composed of technologies that advance transportation safety and mobility and enhance American productivity by integrating advanced communications technologies into transportation infrastructure and into vehicles.	Intelligent Transportation Systems are used provide traffic management centers with traffic information to drive decisions, execute action plans, and operate the roads and equipment.	USDOT: ITS Fact sheet
Internet of Things	IoT	IT	IoT is an instantiation of a network of things (NoT), more specifically, IoT has its ‘things’ tethered to the Internet. A different type of NoT could be a Local Area Network (LAN), with none of its ‘things’ connected to the Internet. Social media networks, sensor networks, and the Industrial Internet are all variants of NoTs.	Devices such as smart lights, in home assistants, and other smart tech are considered IoT devices.	NIST SP 800-183

Term	Acronym	Domain	Definition	Example / Usage	Source
Internet Protocol	IP	Cyber	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.	IP is used for the Internet, as it establishes the rules, protocols, and routing of information over digital networks.	CNSSI-4009-2015, Page 70
Intrusion Detection	-	Cyber	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.	Often this method is implemented using statistical measures, such as recording and comparing timing between messages. For example, if an attacker is sending messages mimicking actual network traffic, but at an increased rate, intrusion detection methods could catch these malicious messages and flag them based on an incorrect rate.	NIST SP 800-94, Appendix A
Intrusion Detection System	IDS	Cyber	Software that automates the intrusion detection process.	This system will often sit on a TMC's network and alert IT staff within the organization of any unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files. Similar to an IPS but does not take any action other than alerting in response to unusual activity.	NIST SP 800-94, Appendix A

Term	Acronym	Domain	Definition	Example / Usage	Source
Intrusion Prevention System	IPS	Cyber	Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Also called an intrusion detection and prevention system.	This system will often sit on a TMC's network and alert IT staff within the organization and attempt to stop/remedy any unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files. Similar to an IDS but attempts to stop unusual activity rather than just alert staff.	NIST SP 800-94, Appendix A
Key sizes	-	Cyber	The length of a cryptographic key in bits; used interchangeably with "Key length." Related term: cryptography.	Typical key sizes are represented as powers of two such as 128, 256, 512, 1024, and 2048. These key sizes are used when implementing algorithms such as AES, in which there are different algorithms for different key sizes (e.g., AES-128, AES-256).	NIST SP 800-57 pt1 r5, Section 2.1
Keylogger	-	Cyber	A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures.	A keylogger was used on the server and captured the administrator's username and password.	NIST SP 800-82 Rev. 2 Appendix B
Kill Chain	-	Cyber	Coined by Lockheed Martin, the Cyber Kill Chain is a framework used for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.	An example kill chain would include: • gaining information about devices on a network from a data breach. • finding a device that has a network vulnerability • finding an exploit for the device • use that device to gain access to the enterprise network.	https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Term	Acronym	Domain	Definition	Example / Usage	Source
Least Privilege	-	Cyber	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	In an organization, all individuals/entities do not need access to all files/resources within that system. For example, an operator does not need access to the firewall rules specified by IT, and thus will not need access as it is not deemed necessary for successful completion of their role.	CNSSI-4009-2015, Page 76
Logic Bomb	-	Cyber	A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.	In 2013, a malicious attacker or group of hackers planted a virus on computers of banks and broadcast agencies. It was programmed to wipe the hard drives and startup instructions for the computers at a precise time. This time-coordinated attack was a logic bomb. Ref: https://www.wired.com/2013/03/logic-bomb-south-Korea-attack/	NIST SP 800-12 Rev. 1 Appendix B
Loop Detector	-	Transportation	A sensor to detect vehicles passing over or stopped within the detection area of an inductive-loop detector. A stopped vehicle decreases the inductance of the loop, and the electronics unit senses this event which sends a pulse to the controller signifying the passage or presence of a vehicle.	Loop detectors are embedded in the roadway and are used for detecting the presence of vehicles on the roadway.	https://www.fhwa.dot.gov/publications/research/operations/its/06108/02.cfm

Term	Acronym	Domain	Definition	Example / Usage	Source
Malware	-	Cyber	Short for malicious software. Synonym(s): malicious code, malicious applet, malicious logic. Software that compromises the operation of a system by performing an unauthorized function or process.	An example of malware may be a worm, virus, ransomware, or trojan that seeks to manipulate a target computer. Malware can also be used to execute phishing, spear phishing, or whaling attacks.	CNSSI-4009, NIST SP 800-83, M Section
Man-in-the-Middle	MitM	Cyber	An attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.	An example of a MitM attack is a USB keylogger that is attached to the keyboard of a server and captures the username and password. An attacker will use this attack often times to get things like passwords, sensitive personal information, or cryptographic keys. Methods like Transport Layer Security (TLS), commonly used in HTTPS when accessing webpages, are used to protect against this attack when information is transmitted over a network. These methods both encrypt data within the message to be sent and verify both the sender and receiver are valid before the message is sent.	https://tools.ietf.org/html/rfc4949

Term	Acronym	Domain	Definition	Example / Usage	Source
Media Access Control	MAC	IT	AKA MAC address. A unique 48-bit number (that is, a number between 0 and 281474976710655) that was programmed into a network interface by the equipment manufacturer at the time of manufacturer, and that distinguishes one device from another on the network. This number is often represented in a two-digit hexadecimal format (numbers 0-9 and letters A-F) with hyphens between the bytes.	For example, the difference between an iPhone and Android device will be evident in the MAC address of the two devices. An iPhone has a MAC address starting F0-99-B6… and an Android has one starting F0-25-B7.	https://www.ftc.gov/system/files/documents/public_comments/2014/03/00019-89125.pdf
Mission Critical	-	IT	AKA Critical Component. Any telecommunications or information system that is defined as a national security system (Federal Information Security Management Act (FISMA) of 2002) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.	For example, in a traffic intersection, a mission critical piece would be the traffic signal controller, as it controls signal operation and timing.	CNSSI-4009-2015, Page 82

Term	Acronym	Domain	Definition	Example / Usage	Source
Multi-Factor Authentication	MFA	Cyber	Authentication using two or more different factors to achieve authentication.	Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Using (i) something you know and (ii) something you have such as a token to access a system is an example of multi-factor authentication.	NIST SP 800-53 Rev. 4 Appendix B
Nation State	-	Cyber	Large, Government-sponsored groups that use cyber espionage as a tool for countering internal dissent or acquiring diplomatic or competitive advantage. Some governments use cyber asymmetry to challenge established powers with significant diplomatic sway or military power or to target private sector entities. Others have latched onto financially motivated cybercrime as a means of evading sanctions.	Examples of attacks leveraged by Nation states include: NotPetya, WannaCry, Destover, and Stuxnext.	https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-Nation-state-actors.pdf

Term	Acronym	Domain	Definition	Example / Usage	Source
National Cybersecurity & Communications Integration Center	NCCIC	Cyber	The central location operated by the DHS Office of Cybersecurity and Communications where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts.	The NCCIC has multiple responsibilities that include: • Build risk awareness and help people understand how to mitigate threats and vulnerabilities. • Help customers take action to improve their risk posture and support a common operational picture of the national cyber and communications risk landscape. • Defend Federal networks and respond to significant incidents. • Defend the Federal Government's critical networks and stand ready to respond to attacks on both Government and private sector networks. If an organization were to be attacked or received information on a cyber event, they would reach out to the NCCIC with all relevant information, which would then disseminate this information to other organizations.	CISA: NCCIC Website

Term	Acronym	Domain	Definition	Example / Usage	Source
National Institute of Standards	NIST	Cyber	The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. Considered to be experts in the publication of cybersecurity best practices.	NIST also provides multiple industries with standards and measurements, as stated on the NIST site "From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology."	https://www.nist.gov/about-nist
National Transportation Communications for Intelligent Transportation System Protocol	NTCIP	Transportation	A family of standards that provides both the rules for communicating (called protocols) and the vocabulary (called objects) necessary to allow electronic traffic control equipment from different equipment manufacturers to operate with each other as a system.	See Appendix D for an example.	https://www.ntcip.org/about
Network Mapping	-	IT	A process that discovers, collects, and displays the physical and logical information required to produce a network map.	Often results in diagrams as a web, with a line between devices representing a connection. For example, if an organization where to document all devices found on their network through tools such as Nmap, this would result in a map of their network. See example of a network map shown Appendix D.	CNSSI-4009-2015, Page 86

Term	Acronym	Domain	Definition	Example / Usage	Source
Network Segmentation	-	IT	AKA micro segmentation. A technique to achieve logical separation for applications with different sensitivity levels or belonging to different departments.	This is often achieved using architecture planning, gateways/firewalls, or virtual local access networks (VLANs) to separate different levels of the network. For example, if an IT group wanted to separate an internal network from an external network, they would implement a VLAN to ensure network segmentation.	NIST SP 800-125B, Section 2
Operational Technology	OT	Transportation	Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. OT supports productions or operational environments. Contrast to Information Technology.	For example, a traffic signal controller will adjust signal timing based on the presence of a vehicle according to cameras or loop detectors. This term is also applicable to Industrial Control Systems (ICS), in that many of the field devices are considered part of an organization's operational technology.	NISTIR 8183 Appendix B
Password entropy	-	Cyber	A measure of password security that represents the amount of uncertainty an attacker faces to determine a password. Often used when discussing the brute-forcing of a password.	For example, the password 1234 would have low entropy while an unpredictable password like 1!3$^aBD32 would have much higher entropy.	NIST SP 800-63-3 Appendix A, Pg. 46
Patch Management	-	IT	The process for identifying, acquiring, installing, and verifying patches for products and systems.	For example, if a workstation needs an update, through patch management procedures, IT personnel will be notified, and will then perform needed updates.	NIST SP 800-43 r3, Abstract

Term	Acronym	Domain	Definition	Example / Usage	Source
Penetration Testing	-	Cyber	AKA pen testing. Security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.	Typical penetration testing are typically composed of multiple stages: • Identification of devices to be tested • Service enumeration (e.g., network services, open hardware ports, and serial interfaces.) • Planning of attacks against these devices (e.g., replaying messages to serial port, unauthorized access) • Execution/documentation of attacks • Reporting on tests, usually in the form or a report with pass/fail measurements. Pen testing is often split into two types: Ethical and Unethical. Ethical—Testing with expressed permission from the party to be tested. Often performed by security researchers. Unethical—Testing without expressed permission and is often performed for personal or agenda gain. For example, an organization may perform a penetration test on their systems to ensure that they are following proper and secure protocols.	NIST SP 800-115, Appendix F

Term	Acronym	Domain	Definition	Example / Usage	Source
Persistence	-	Cyber	Techniques that CTAs use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.	An example of a persistent attack is seen in Stuxnet, in that the attackers pursued their objective to destroy the Iranian nuclear centrifuges repeatedly over an extended period of time.	https://attack.mitre.org/tactics/TA0003/
Personally Identifiable Information	PII	IT	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, and (2) any other information that is linked or linkable to an individual.	Includes data such as name, social security number, date and place of birth, mother's maiden name, and records such as medical, educational, financial, and employment information.	NIST SP 800-122 Appendix E

Term	Acronym	Domain	Definition	Example / Usage	Source
Phishing	-	Cyber	A technique for tricking individuals into disclosing sensitive personal information by claiming to be trustworthy entity in an electronic communication (e.g., Internet websites).	Phishing attacks utilize brand recognition and well-known services, such as banks, law firms or social networking sites, to encourage the largest number of people to take some action causing them to share sensitive information such as credit card, social security number or account information (i.e., username/password). There is usually some sense of urgency to the email so that the recipient will respond, hopefully, without thinking critically. For example, they may send out an email from a well-known bank stating that it is conducting a routine account verification process and could not validated the user's information. It will then request the user to click on link within an urgent timeframe to ensure the user's account remains active. Legitimate organizations will never request this via email.	NIST SP 800-82 r2, Appendix B
Physical Security	-	Transportation	Also referred to as Physical Access Controls Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment, and resources, and to protect personnel and property from damage or harm.	A physical lock (combination, magnetic, or key) or enclosure/building. In a typical traffic intersection setup, this would be the locked traffic cabinet that houses the rest of the components. See Access Control—Physical	NIST SP 800-53 Rev. 4 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Policy	-	Cyber	The statements, rules or assertions that specify the correct or expected behavior of an entity. Can also refer to specific security rules for a system or even the specific managerial decisions that dictate an organization's email privacy policy or remote access security policy.	An example policy may dictate what actions a firewall is to take when receiving a new connection to the network or sees traffic on a network.	NIST SP 800-12 r1, Section 5
Port Scan	-	Cyber	Sending client packets or requests to a range of service port addresses on another host system.	Individuals and network administrators perform port scans to identify potential security holes on the system. Cyber attackers perform port scans to learn of potential vulnerability points that may be exploited. Port scans may be performed as active or passive, depending on whether they interact with devices on the network while scanning.	CNSSI-4009-2015, Page 95
Port Scanner	-	Cyber	A program that can remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).	NMAP is an example of a port scanner with extensive functionality. For example, using the -O flag with the Nmap tool will also return the OS of the contacted device, one of the many interesting features available.	NIST SP 800-115 Appendix F

Term	Acronym	Domain	Definition	Example / Usage	Source
Privacy	-	IT	The assurance that the confidentiality of, and access to, certain information about an entity is protected.	For example, if one were to send a PII data to another person (e.g., hospital, physician), they would want no one else who is not meant to see this message to be able to view the message contents. This is the key principle behind privacy.	CISA: NICCS Glossary, Section P
Profile	-	Cyber	A representation of the outcomes that a particular system or organization has selected from the NIST Cyber Security Framework Categories and Subcategories. An organization's target profile is the desired outcome or "to be" state of cybersecurity implementation, while the current is the "as is" state of system security.	A security profile may include things like: • use of encryption • use of firewalls • use of antivirus software The use of the items listed above may help determine what activities to activities to prioritize. For example, if an organization wanted to ensure confidentiality of information and did not have TLS enabled on web traffic within their systems, they would prioritize TLS to ensure confidentiality of data in motion.	NIST IR 8183, Appendix B
Protect	-	Cyber	Part of the NIST cybersecurity framework core functions. To implement procedures that guard against cyber threats and attacks.	For example, an organization may reference their security profile and implement lacking aspects to better protect their systems.	https://www.nist.gov/cyberframework/protect

Term	Acronym	Domain	Definition	Example / Usage	Source
Public Key Certificate	-	Cyber	A data structure that contains an entity's identifier(s), the entity's public key (including an indication of the associated set of domain parameters), and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e., a certificate authority thereby binding the public key to the included identifier(s).	The standard that defines a certificates format is X.509, which are implemented in Internet protocols such as TLS/SSL and HTTPS.	NIST SP 800-56A Rev. 3 Section 3.1
Public Key Infrastructure	PKI	Cyber	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.	Website URLs utilize Public Key Infrastructure to secure HTTPS connections by using a public/private key structure. This leverages the advantages of asymmetric key cryptography. DigiCert is a main provider for the public key certificates. Additionally, Security Credential Management System (SCMS) is a proof-of-concept message system that uses a PKI approach for large-scale distribution of certificates for Connected Vehicles (CV).	CNSSI-4009-2015, Page 99, https://www.its.dot.gov/resources/scms.htm

Term	Acronym	Domain	Definition	Example / Usage	Source
Ransomware	-	Cyber	Malware, or malicious software, that encrypts data stored within a system, and demands payment for decryption of that data.	Ransomware is typically part of a cyber-attack on one or more computers, spreading through phishing emails or unknowingly visiting infected websites. An example of a cyber-attack using ransomware would be the SamSam attack that halted services within the Colorado Department of Transportation (CDOT) in February 2018. A threat actor took advantage of misconfigured virtual servers to gain access to the state's network and loaded the ransomware, encrypting the state's data business computers and requesting payment in order to decrypt and release them. It took weeks for the state to remove the threat and restore service. [https://searchsecurity.techtarget.com/news/252479128/Colorado-CISO-details-SamSam-ransomware-attack-recovery]	NIST SP 1800-26 [DRAFT], Section 1.1

Term	Acronym	Domain	Definition	Example / Usage	Source
Recover	-	Cyber	Part of the NIST cybersecurity framework core functions. The development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber incident.	Recover is an activity to be performed not only following a cyber incident to restore any capabilities or services that were impaired, but it is also an activity to improve an organization's' and/or systems' resiliency to future incidents through the development of recovery plans and communication channels. For example, in the SAMSAM ransomware cyber incident, CDOT was able to restore its business operations, and improve its security practices to reduce the chance of a similar attack occurring. It also allowed revealed communication paths and courses of action that aided the development of recovery plans for timely response to future cyber incidents.	NIST Framework V1.1, section 2.1;
Red Team	-	Cyber	Often times used as a verb i.e., red teaming A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture.	The Red Team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.	CNSSI-4009-2015, Page 101

Term	Acronym	Domain	Definition	Example / Usage	Source
Resilience	-	Cyber	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	To be resilient, an organization should consider the likely risk associated with implementing a given process/action. Doing so, these processes are called risk-aware processes. For example, when adding a device to a network, if an organization first researches the device and consider potential vulnerabilities associated with that device, they are considered risk-aware, which leads to resilience.	CNSSI-4009-2015, Page 103
Respond	-	Cyber	Part of the NIST cybersecurity framework core functions. The development and implementation of appropriate activities to take action regarding a detected cybersecurity incident.	When an organization discovers/falls victim to a cyber incident, they can respond by communicating to affected parties, analyzing the incident and prescribing mitigating actions to reduce impact of the incident. For these activates to be effectively carried out, a response plan should be developed describing their implementation and updated from lessons learned following a cyber incident.	NIST Framework V1.1, section 2.1

Term	Acronym	Domain	Definition	Example / Usage	Source
Risk	-	Cyber	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Often expressed as the formula Risk = Threat x Vulnerability x Consequence	An example risk to a network could be allowing BYOD (bring your own device), given that there will be limited control as to what software is loaded on the device and the software may introduce viruses that could compromise other systems.	NIST SP 800-53 Rev.4 Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Risk Analysis	-	Cyber	AKA risk assessment. The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.	When performing a risk analysis, organizations may take into field device risk assessments, IT device risk assessments, and overall network risk assessments that have been performed. Based on these different assessments, an organization will effectively be able to assess risk associated with assets in their organization.	NIST SP 800-39, Appendix B
Risk Management	-	Cyber	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.	For example, this could be implementing firewall or other system changes based on the result of a risk analysis.	NIST SP 800-39, Appendix B

Term	Acronym	Domain	Definition	Example / Usage	Source
Scanning	-	Cyber	AKA Vulnerability Scanning. Sending packets or requests to one or more service port addresses on another system to gain information to be used in a subsequent attack.	Scanning itself is usually a benign activity. It is an inspection of available systems, and subsequent ports and services. How its information is used determines if the intent is malicious. Individuals and network administrators perform inspections to identify potential security holes on systems and/or networked devices. Cyber attackers perform scanning to learn of potential vulnerability points that may be exploited.	CNSSI-4009-2015, Page 106
Secure Sockets Layer	SSL	Cyber	A security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	Used to secure connections and data in transit prior to the adoption of TLS. Currently, all versions of SSL are considered deprecated, and TLS should instead be used.	https://tools.ietf.org/html/rfc6101
Security Awareness	-	Cyber	Programs and training that provide IT users knowledge in security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources.	For example, a security training course required for all members of an organization.	NIST SP 800-50, Executive Summary

Term	Acronym	Domain	Definition	Example / Usage	Source
Security Researcher	-	Cyber	AKA Computer Security Researcher; AKA Cybersecurity Researcher; AKA Network Security Researcher; AKA Ethical Hacker; AKA White Hat Hacker; AKA Certified Ethical Hacker (CEH) Someone who conducts research into security vulnerabilities that exist in software applications, hardware, attempts to discover and reverse engineer malware, and finds flaws in websites and commonly used Internet protocols. Often, this term is the preferred naming of ethical hackers and pen testers.	For example, a security researcher will investigate vulnerabilities on a certain embedded device for the purpose of better securing that device. Then, after discovering a vulnerability, will usually disseminate this research in an ethical manner to any number of stakeholders (e.g., Government, corporate, public, or a mix).	No official reference but a commonly used jargon. https://www.secplicity.org/2018/11/21/security-researcher-track-101/ ; https://www.eff.org/pages/grey-hat-guide
Separation of Duties	-	Cyber	A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud.	Using the example of an operator, an operator may be the expert in a device's configuration but will not be an expert on the configurations of workstations in a TMC.	NIST SP 800-57 Part 2 Section 1.5.1

Term	Acronym	Domain	Definition	Example / Usage	Source
Social Engineering	-	Cyber	The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.	Social engineering is the science of skillfully maneuvering social interactions to get another person to take some kind of action. It is practiced informally and by professionals such as teachers, lawyers, doctors, and many others to gather information or coherence a patient, client, student to perform some task. A simple example would be getting a discounted or free coffee from one's favorite coffee shop. From a cybersecurity perspective, an individual may use this tactic to gather personal or company-confidential information in order to gain unauthorized access to a system or network.	NIST SP 800-63-3 Appendix A
Spoofing	-	Cyber	Faking the sending address of a transmission to gain illegal entry into a secure system and/or to mask an attacker's true identity.	Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. For example, impersonating another device’s hardware identifier (e.g., Media Access Channel address) allows an attacker to circumvent access control.	CNSSI-4009-2015, Page 116

Term	Acronym	Domain	Definition	Example / Usage	Source
Spyware	-	Cyber	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.	A well-known example of spyware is a key logging program in which a user's keystrokes are either logged or sent to an attacker's PC. Spywares are often used in conjunction with other methods (i.e., viruses, bot, trojan) for a means of transmission. Spyware is not limited to key logging, and may be also used in voice, video, or activity tracking.	NIST SP 800-53 Rev.4 Appendix B
Supervisory Control and Data Acquisition	SCADA	Transportation	A system used to control dispersed assets where centralized data acquisition is as important as control	SCADA systems are computer systems used to monitor, control, and analyze real-time data on industrial equipment such as telecommunications, water and waste control, energy, oil and gas refining and transportation. A transportation example of SCADA is seen in a TMC that sends commands to field devices and receives operational data back from these field devices.	NIST SP 800-82 Rev.2 Appendix B
Supply Chain Risk Management	-	Cyber	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology (ICT) product and service supply chains	For example, a sample section of a supply chain that needs security is the procurement of field devices by a TMC. If the purchasing portion of the activity is unsecured, an attacker may intercept sensitive information that would allow them to make purchases on behalf of the TMC or even simply steal the account details. Supply chain security is often a combination of both physical and cyber security.	NIST SP 800-161, Glossary

Term	Acronym	Domain	Definition	Example / Usage	Source
System Backup	-	IT	The act of copying information or processing status to a redundant system, service, device, or medium that can provide the necessary processing capability when needed.	There are many implementations of this process, and typically will depend on what system the user is backing up. For example, if a user wanted to back up their personal system, they could use a tool like Windows Backup included with Windows 10 to backup. Also, if the backup of data were to fail, the status (e.g., 50% complete) will also backup to preserve processing status. Many systems and concepts are used to support system backups including failovers, VM migration, and physically distant backups.	NIST SP 800-152 Appendix B
Threat	-	Cyber	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	Often threats are deemed as such with either a user of the system, the organization, or to the public as a whole in mind. When an organization performs a threat assessment, they first identify threats like unencrypted network traffic or lack of antivirus software, and then determine the impact that this threat may cause.	CNSSI-4009-2015, Page 115
Threat Actor	-	Cyber	See Cyber Threat Actor for definition.	-	-

Term	Acronym	Domain	Definition	Example / Usage	Source
Threat Intelligence	-	Cyber	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.	Often this is the final product of a threat assessment, which is presented to leaders at the top level of an organization so that they can make decision to address the threats identified.	NIST SP 800-150 Appendix B
Traffic Light Protocol	TLP	Cyber	TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. TLP was created in order to facilitate greater sharing of information in the computer security incident response team (CSIRT) community. It is currently used by Federal entities such as NCCIC and CISA to share cyber incident information.	TLP was setup to enable information sharing and indicts information's sensitivity along with who is the appropriate audience. TLP is used within various organizations, such as transportation ISACs, to disseminate cyber incidents and prevention and response information. See Appendix D for a graphical representation.	CISA: TLP Definitions and Usage
Traffic Management Center	TMC	Transportation	A center or hub for gathering and sharing information, making operational and management decisions, and implementing control strategies to affect these decisions. Synonymous with Transportation Management Center.	TMC is used as the physical location where the traffic operators are stationed.	FHWA: Freeway Management and Operations Handbook, Chapter 14

Term	Acronym	Domain	Definition	Example / Usage	Source
Traffic Management System	TMS	Transportation	Traffic Management Systems are a field of the Intelligent Transportation Systems (ITS) and are typically deployed as software services. These systems perform the function of monitoring, controlling, and managing the functional elements of a transportation management system through the use of computers and computer networks without having a presence at a physical nerve center or without the existence of such a physical nerve center.	An example of a TMS is used by organizations such as TxDOT, or other state and municipality Departments of Transportation. For TxDOT, a TMS can stream real-time transportation data from the entire traffic infrastructure into one Transportation Management Center (TMC). The TMC then processes the data and takes intelligent actions that increase transport efficiency, mitigate traffic congestion, and improve safety.	https://ops.fhwa.dot.gov/publications/fhwahop14016/fhwahop14016.pdf
Traffic Signal Controller	-	Transportation	Also referred to simply as Controller. A device usually mounted at an intersection that is responsible for controlling the traffic signals at an intersection to ensure that traffic and pedestrians move as smoothly and safely as possible. A conflict monitor is typically a separate component that operates with the traffic signal controller and is responsible for preventing crashes by verifying that the lights will not cause crossing vehicles to enter the intersection at the same time.	An example of a traffic signal controller would be Econolite's Cobalt https://www.econolite.com/products/controllers/cobalt-rackmount/	FHWA: Traffic Control Systems Handbook, Chapter 7

Term	Acronym	Domain	Definition	Example / Usage	Source
Transport Layer Security	TLS	IT	Protocol that allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery. Created to replace the deprecated SSL. Related term: SSL.	Transport Layer Security (TLS) protocols are used to secure communications in a wide variety of online transactions, such as financial transactions (e.g., banking, trading stocks, e-commerce), healthcare transactions (e.g., viewing medical records or scheduling medical appointments), and social transactions (e.g., email or social networking). Any network service that handles sensitive or valuable data, whether it is PII, financial data, or login information, needs to adequately protect that data. Contrast to encryption, which provides message-level security.	https://tools.ietf.org/html/rfc8446
Transportation Management Center	TMC	Transportation	Also known as Traffic Management Center, tactical operations center (TOC) or back office. A central facility that controls, monitors, and manages the surface street, highway, transit, and bridge/tunnel control systems within its control area.	An example of a TMC is an organization such as TxDOT, or other state and municipality Departments of Transportation.	FHWA: Freeway Management and Operations Handbook, Chapter 14

Term	Acronym	Domain	Definition	Example / Usage	Source
United States Computer Emergency Readiness Team	U.S.-CERT	Cyber	A partnership between the DHS and the public and private sectors, established to protect the Nation's Internet infrastructure. U.S.-CERT coordinates defense against and responses to cyber-attacks across the Nation. Often collaborates with ICS-CERT.	U.S.-CERT's main mission is to act as a global information exchange hub. This means that when an organization has a cyber event, they report it to U.S.-CERT so that other organizations can be prepared and have the proper defenses in place for such an attack.	CNSSI-4009-2015, Page 130
Virtual Private Network	VPN	IT	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.	An individual in a TMC will often use a VPN to either access the TMC from an external source or access external (i.e., field) devices from the TMC. The importance of a VPN is its focus on a secure connection, even when connecting to the outside Internet.	NIST SP 800-82 Rev. 2 Appendix B

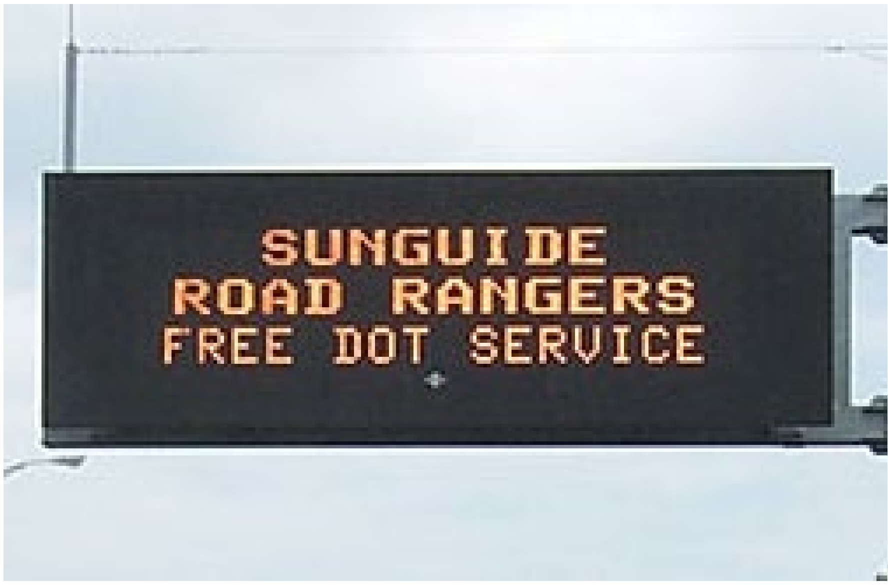
Term	Acronym	Domain	Definition	Example / Usage	Source
Virus	-	Cyber	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.	Well-known examples of viruses include Cryptolocker, WannaCry, ILOVEYOU, and MyDoom. Each of these affects user files when they run the virus, either encrypting or holding the files until a sum of money is paid, or outright deleting or modifying the files. Antivirus software will often catch a virus before causing damage to a system.	NIST SP 800-82 Rev. 2 Appendix B
Vulnerability	-	Cyber	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	A simple example of a vulnerability would be an open network port on a firewall that allows attackers access to the network.	NIST SP 800-37 Rev. 2 Appendix B
Vulnerability Scanning	-	Cyber	See Scanning.	-	-

Term	Acronym	Domain	Definition	Example / Usage	Source
White Team	-	Cyber	The group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results.	For example, a white team may consist of previous members of red and blue teams, as they will be familiar with the methods of both as well as the rules of engagement.	CNSSI-4009-2015, Page 132

Term	Acronym	Domain	Definition	Example / Usage	Source
Whitelist	-	Cyber	A list of applications and application components that are authorized for use in an organization.	This list is often used with applications such as firewalls and antivirus and will referenced when a host or application tries to perform an action on the network.	NIST 800-167, Abstract
Wireless Network Security	-	Cyber	The protection of wireless networks through the use of cybersecurity processes.	Examples include Wired Equivalent Privacy WEP (which is considered insecure), Wi-Fi Protected Access (WPA which is also considered insecure), and Wi-Fi Protected Access-2 (WPA2 which is preferred to either of the previous security protocols).	NIST SP 800-153, Executive Summary
Zero-day attacks	-	Cyber	An attack that exploits a previously unknown hardware, firmware, or software vulnerability. A zero-day vulnerability is one that has no patch available that would address the vulnerability.	Well-known examples of zero-day attacks include: Stuxnet, Aurora, and the RSA hack. These attacks are often unknown to antivirus software.	CNSSI-4009-2015, Page 133
Zombie	-	Cyber	A zombie is a program which is installed on a host that has the ability it to attack other hosts.	Similar to a bot, however while bots can be used for non-malicious tasks such as by search engines to collect webpage information, zombies are considered to only be used for malicious tasks.	NIST SP 800-83 r1, Section 2.2

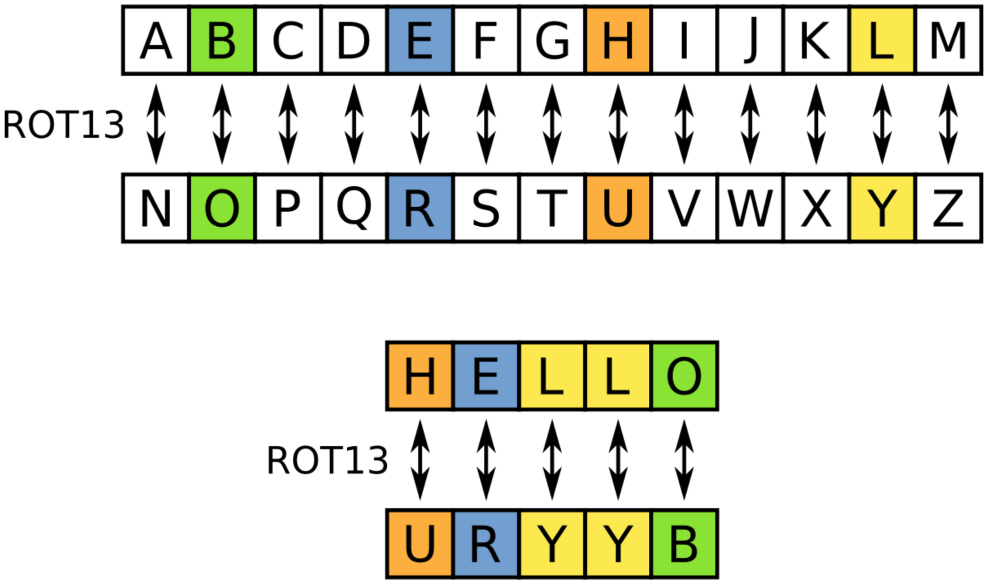
Appendix D. Terminology Figures

The following figures are used as examples of the terminology defined in Appendix C.



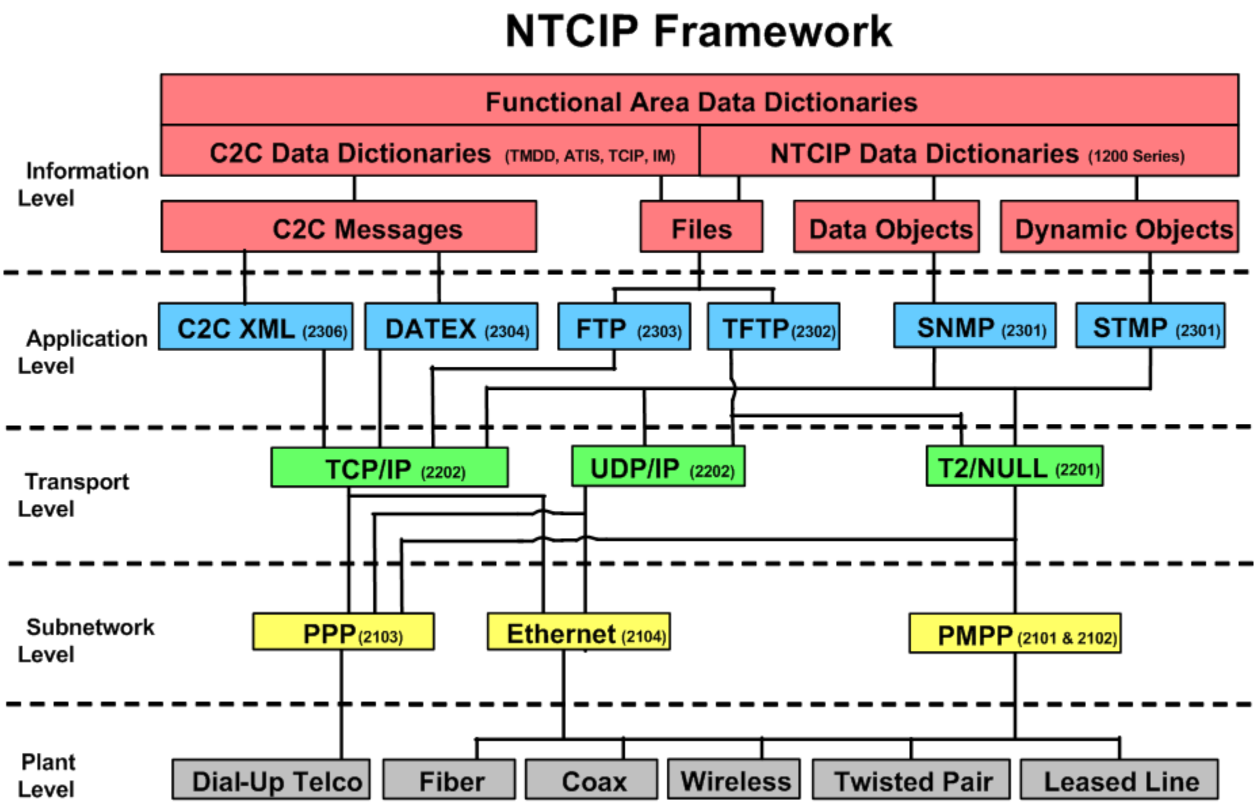
Source: Provided by FDOT **https://sunguide.info/its-program/dynamic-message-signs-dms/**

Figure 18. Photograph. Example of Dynamic Message Sign.



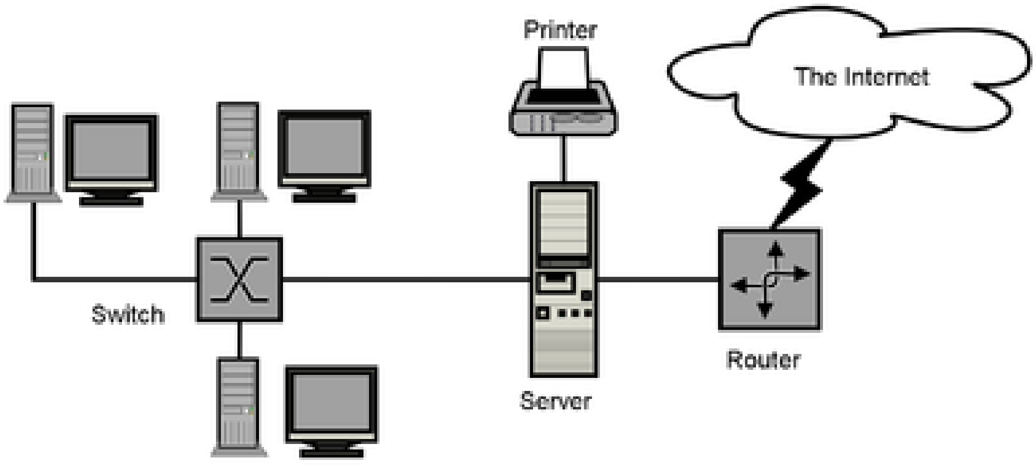
Source: Image is in the public domain **https://en.wikipedia.org/wiki/Public_domain**

Figure 19. Diagram. Example of encryption using ROT13.



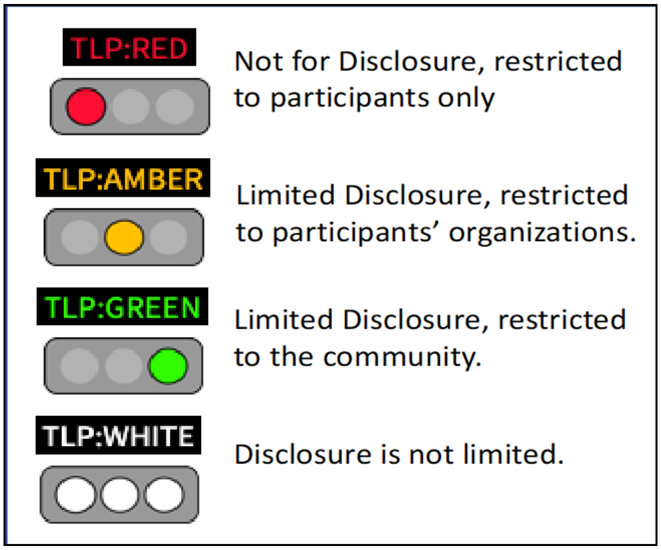
Source: Reprinted from NTCIP 9001 v04 'The NTCIP Guide' by permission of NEMA. Re-use by permission of NEMA. No changes made. CC BY-SA 3.0 ***https://creativecommons.org/licenses/by-sa/3.0/***

Figure 20. Diagram. National Transportation Communications for Intelligent Transportation System Protocol framework.



Source: Reprinted from NTCIP 9001 v04 'The NTCIP Guide' by permission of NEMA. Re-use by permission of NEMA. No changes made. CC BY 2.5 ***https://creativecommons.org/licenses/by/2.5/***

Figure 21. Diagram. Network mapping example.


TLP:RED
Not for Disclosure, restricted to participants only
TLP:AMBER
Limited Disclosure, restricted to participants' organizations.
TLP:GREEN
Limited Disclosure, restricted to the community.
TLP:WHITE
Disclosure is not limited.

Source: FHWA

Figure 22. Illustration. Traffic light protocol example image.

Appendix E. Example Rubrics Supporting Success Criteria

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 Game Master (GM) will note that a "turn," also sometimes called a "step," 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 each 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 ISAOs. In this example, the participant will be docked points for not beginning their IMP or effectively communicating (e.g., reaching out to their CISO).

Exercise 1. Results—Rubric

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	-

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
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	-	1-5: +3 points 6-10: +5 points 11-20: +1 Never: 0	-
Contact System Integrators/Contractors	3	3-6: +3 points 8-12: +5 points 13+: +1 1-2: -5 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	-

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
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	-
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	-

Fusion Center/MS-ISAC Rubric			
Action	**Turn**	**Comments**	**Points**
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	-
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	-

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	-

Exercise 2. Results—Rubric

The following are the rubrics used to assess the performance of participants during the first exercise. See Appendix E 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	-
Contact Equipment Manufacturer	2	4-7: +3 points 9-13: +5 points 14+: +1 1-3: -5 Never: 0	-5**

Municipal IOO Rubric			
Action	**Turn**	**Comments**	**Points**
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: -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] Unique to this scenario, LE many not be needed in other scenarios.

** Note that -5 points were given from an action being taking too soon. Contacting the equipment manufacturer or an external source prior to confirming the vulnerability and contacting the Municipal/State CISO can have adverse effects on incident response process.

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	-
Contact State CISO	2	1-5: +5 points 6-10: +3 points 11-20: +1 Never: 0	5

State IOO Rubric			
Action	**Turn**	**Comments**	**Points**
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	-
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	-
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	-

Municipal 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	-

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	-

State CISO Rubric			
Action	**Turn**	**Comments**	**Points**
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	-
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	-

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-21-851

U.S. Department of Transportation