Incident Response Plan Tabletop Exercise	Date	4/2/2025

	Printed Name	Signature
1	Kelly Casas /CISA	
2	Shelly Jones / COD-TS	Shelly
3	Gregory Wolfe / COD-TS	Greg Wolfe
4	Alyssa Owen	
5	Bob Martinez	
6	Tony Jones	
7	Christian Matt	
8	Elizabeth Coulter	Elizabeth A Coulter
9	PAUL DESJARDINS	
10	Cameron Zahn	
11	Marcella Lunn	Marcella Lunn
12	Azura Kerr	
13	Jerry Looper	
14	Stuart Birdseye	
15	Jonathan Love	
16	Paul Fountain	
17	Jose GAYTAN	
18	Thomas Parks	Thomas Parks Jr
19	Gia Patel	
20	Daniel Pollak	
21		
22		
23		
24		
25		
26		
27		
28		

Exercise Logistics

- Location: 1685 Spencer Rd, Denton TX
- Date: 2 April 2025
- Time: 12:00 pm – 2:00 pm
- Next Meeting: Planning Meeting –

Denton Municipal Electric Cyber Tabletop Exercise (CTTX)

4/2/2025

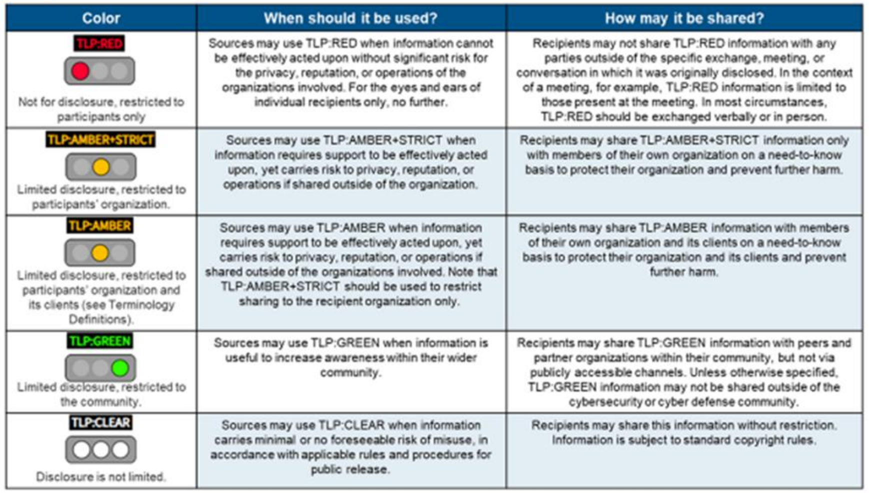
Welcome and Overview

Cameron Zahn
Outage Management and Compliance Supervisor

Exercise Security

TLP:AMBER

The exercise documents are designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.



Color	When should it be used?	How may it be shared?
TLP:RED ●○○ Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT ○●○ Limited disclosure, restricted to participants' organization.	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ○●○ Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ○○● Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ○○○ Disclosure is not limited.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

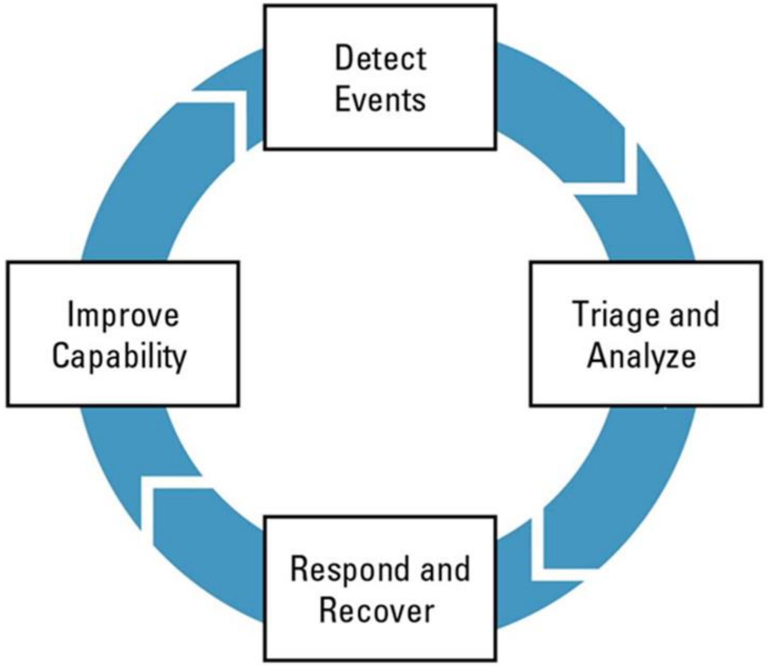
For reference purposes and additional information on TLP: https://www.cisa.gov/tlp

Operations Security (OPSEC)

- Please be aware of the management of the information and documents you obtain today.
- Be aware of public conversations and do not release any of the information discussed today to media sources (e.g., internet)
- This briefing contains exercise, operational, and potentially business sensitive material which, while not classified, should be safeguarded as appropriate.

Scope

This will be a two-hour non-technical facilitated Cyber tabletop exercise, where players are presented with a cyber-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans. The goal of the exercise is identifying strengths and areas for improvement for the Cyber Incident Response Plan.



Exercise Objectives

1. Identification of key regional and local critical infrastructure stakeholders and facilities.
2. Review of incident reporting, intelligence threat warning, and information sharing and dissemination processes between state, local, tribal, and territorial entities; law enforcement; facility owners and operators; and federal departments and agencies in relation to a credible threat to, a security incident at, or attack on, regional or local critical infrastructure.
3. Discuss regional and local stakeholders' emergency preparedness plans and procedures to a security incident or attack on an electric substation and the coordination of activities under the National Incident Management System (NIMS) with federal, state, local, tribal, and territorial entities.
4. Identify gaps in the Cyber Incident Response Plan (CIRP), and procedures in response to a cyber incident

Agenda

Item	POC
Welcome	Cameron Zahn
Administrative and TTX Guidelines	Kelly Casas
Introductions	
Security Briefing	Chad Johnson
Module 1	Kelly Casas
Break	
Module 2	Kelly Casas
Hotwash	Kelly Casas/Chad Johnson
Closing Remarks	Cameron Zahn

Introductions

- **Name**
- **Title**
- **Organization**

Security Briefing

Chad Johnston
Protective Security Advisor-North Texas
Cybersecurity and Infrastructure Security Agency
Integrated Operations Division-Region 6

Exercise Roles

- **Players** are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency. They respond to the situation presented based on current plans, policies, and procedures.

- **Observers** do not directly participate in the exercise; however, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

- **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.

- **Data Collectors** observe and record the discussions during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

- Each module will begin with an update summary of key scenario events.
- Participants will then engage in issue-based discussions.
- The facilitator will manage time allotted for each discussion period.
- The exercise will conclude with a participant Hot Wash.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Participants should expect varying viewpoints, even disagreements.
- Respond to the scenario using your knowledge of current plans and capabilities and insights derived from your understanding of plans, policies, and procedures.
- Decisions are not precedent setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommendations that could improve response and recovery efforts. Exercise participants will benefit most when they focus on problem solving efforts.

Assumptions & Artificialities

- The adversary and events are fictional and do not reflect actual intelligence.
- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated, not the participants.
- The exercise scenario is plausible, and events occur as they are presented.
- There are neither “hidden agendas” nor any “trick questions.”
- All players receive information at the same time.

Module 1: Incident Identification

Within the DME Service Station Area

Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) and partner agencies release an alert detailing a confirmed compromise of IT and operational technology (OT) networks of a U.S. electric utility provider by a state-sponsored cyber actor. The threat actor used multiple techniques to gain access to IT/OT networks, including exploiting known vulnerabilities, obtaining valid administrator credentials through privilege escalation vulnerabilities and exfiltration of the Active Directory, and living off the land techniques to maintain persistence. CISA assesses with high confidence that state-sponsored actors intend to compromise additional IT/OT networks within the DME Substation Service area.

Module 1: Questions

1. What are the greatest cyber threats to your organization?
    a. What are the possible impacts of an intrusion into your systems?
2. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
    a. What IT and OT systems or processes are the most critical to your organization?
    b. What improvements were implemented to enhance cyber resilience following recent risk assessments?
3. What cybersecurity threat information does your organization receive?
    a. What are your primary sources of information?
    b. How do you determine what information is relevant to your equipment and operations?

Module 1: Questions cont.

Day 6

An IT employee notices a remote desktop protocol window open on their device without any user input. The window closes shortly after it opens, and the employee attributes the issue to a recent update completing its install and takes no further action.

Day 7

One of your third-party vendors releases a patch for a known exploited vulnerability in their devices. They provide edge devices (e.g., firewalls, routers) for your organization. IT is working to implement the patch on the appropriate devices and estimates the patch will be applied to all impacted devices in the next 48 hours.

Day 8

Members of your finance department receive an email that appears to be from the Director of Finance. It instructs them to access a PDF containing details about an unpaid bill from a third-party vendor. Several employees call the Director to verify the email’s authenticity. She replies that she did not send it, and that there is no outstanding vendor bill. Nevertheless, some employees still open the PDF.

Module 1: Questions cont.

1. Describe your organization’s cybersecurity training program for employees.
   a. How often are employees required to complete this training?
   b. What additional training is required for employees who have system administrator-level privileges?
   c. What additional training is required for employees who have access to OT systems?

2. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
   a. What actions does the IT department take when suspicious emails are reported?
   b. What feedback do employees receive after reporting a suspicious email or event?

3. What tools (e.g., threat hunting, security audits) do you leverage as part of a proactive cybersecurity strategy?
   a. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?

Module 1: Questions cont.

4. Describe your organization’s patch management and vulnerability management plans.
    a. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
    b. Describe your policies on remote access to your organization’s network.
    c. What security protocols, such as Multi-Factor Authentication (MFA) and encryption, exist on your hardware?
5. What is the role of cybersecurity in the review and selection of third-party vendor support?
    a. What cybersecurity language (e.g., cybersecurity training and cyber incident notification requirements) is included within third-party vendor contracts?
    b. How do you evaluate the cybersecurity posture of your vendors?
    c. How often are contracts reviewed?

Module 1: cont.

Day 11

IT observes multiple attempts to gain access to your organization’s networks. Threat actors are attempting a variety of attacks based upon legacy edge devices present within your network. The malicious actors are also repeatedly executing distributed denial-of-service (DDoS) attacks against your organization. Upon further investigation of the system logs, they discover that a firewall misconfiguration was noted in the SCADA system.

Module 1: Questions cont.

1. Describe your organization’s approach to managing the lifecycle of critical equipment.
   a. How do you obtain new or replacement equipment?
   b. How do you continue to provide services to your customers while waiting for new/replacement equipment?
   c. Does your organization have any memorandums of understanding or mutual aid agreements with sector partners to maintain services if your equipment fails or is damaged?
2. How does your organization baseline network activity on IT and OT networks?
   a. How do you distinguish between normal and abnormal traffic?
   b. What are your next steps when abnormal activity is detected/reported?
   c. What Indicator of Compromise (IOC) feeds does your organization use?

Module 1: Questions cont.

3. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.
    a. How is physical security integrated into IT and OT security?
4. What are your response priorities?
    a. What actions do you take in response to multiple unauthorized attempts to access your networks and systems?
    b. How would you address the DDoS attacks?
    c. What other protective actions are needed to safeguard your organization?

Break

10 Minute

Break

Module 2:

Day 13 am

- As employees arrive back to work and log in, a red screen appears on workstations. Printers across the Denton Municipal network printed a detailed ransom note:

- All your critical data has been encrypted, and your SCADA operations are now under our control. To regain access to your data and systems, you must pay a ransom of $1,000,000 Bitcoin to the following address: **37bSzXvlKLpTsHMrzb82f617cV4Srnt72S**.

Failure to comply within 72 hours will result in the permanent loss of your data. Any attempts to remove the ransomware or contact authorities will lead to immediate data destruction.

Module 2:

Day 13 pm

It appears a cybersecurity incident impacts your organization ability to submit the day's upcoming submissions for the Energy Management Organization. Employees are unable to access information databases, and internal communication methods such as instant messaging and phone lines are not functioning. Dispatching service personnel for maintenance tasks using the normal methods becomes all but impossible. Devices such as electronic locks and thermostats are also no longer functioning throughout your organization.

Module 2: Questions

1. Discuss your organization’s procedures for declaring a cyber incident.

    a. What escalation criteria are defined in your cyber incident response plan (CIRP)?

2. What alternate communication methods does your organization have if primary systems are unavailable?

    a. How are personnel dispatched to maintenance locations using alternate methods?

    b. How often are alternate communication methods tested and verified?

3. What manual methods for monitoring physical security and safety can you employ if devices such as electronic locks and thermostats are no longer functioning?

Module 2: Questions

4. Do your organization’s emergency response plans (e.g., site security plans, emergency evacuation plans, emergency action plans, or other appropriate plans) contain protocol for properly responding to incidents described in this module?

a. How often does your organization review its emergency response plans, and does it perform drills to test their effectiveness?

b. Do your organization’s response plans address how to coordinate power restoration priorities?

c. Do your organization’s response plans account for law enforcement evidence-gathering requirements?

d. Have cross-sector dependencies been incorporated into your organization’s response plans?

e. Have resulting impacts or cascading effects on other electricity components within the Energy Sector been incorporated into your organization’s response plans?

Module 2 Questions

5. What information sharing processes would you use to disseminate information concerning this incident?
   a. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools, or HSIN) would you use to share information and communicate protective measures implementation?
   b. How would employee safety concerns be managed (e.g., at what point would the utility company allow employees to enter the site)?
   c. What are your organization’s external information sharing responsibilities in response to this incident?
   d. How would proprietary information concerns be managed?
   e. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?

Module 2: Questions

6. What protective security measures would be employed following a domestic attack?
   a. Would you coordinate protective measure implementation with any organization within the Electricity Subsector or specific government entities, such as law enforcement agencies and your CISA PSA?
   b. Would you need to communicate implemented protective measures to organizational liaisons, response entities (e.g., Joint Field Office Unified Command), or other industry or government partners (e.g., Public Utility Commissioner)?
   c. How useful are the information bulletins and advisories the U.S. Department of Homeland Security (DHS) provides (e.g., a JIB) that recommend protective measures?

7. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance)?

8. How would you coordinate public messaging concerning the continuing credible threat to your organization and stakeholders?
   a. What organizations would you coordinate this messaging with?

Module 2: Questions

9. Explain your organization’s decision-making process regarding ransomware payment.
   a. Are ransomware policies/procedures included in your CIRP?
   b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
   c. Discuss the advantages and disadvantages of either agreeing or refusing to pay.
   d. Describe the impact the sale or release of sensitive information or PII would have on your response and recovery activities.
   e. Discuss potential legal and reputational ramifications of paying or not paying the ransom.

10. What capabilities and resources are required for responding to this scenario?
    a. What additional resources outside of your organization would be necessary for responding to the cyber incident?
    b. What are the processes or procedures for requesting additional resources?
    c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?

Module 2: Cont.

Day 14 – Afternoon

Customers are posting on social media that they have lost power to their homes. A few posts include videos of what appears to be a transformer exploding. News media reports on the outages and contacts your organization for comments.

Module 2: Questions Cont.

1. How do IT and OT security teams coordinate incident response efforts?
2. What alternate systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    a. Who can authorize the use of alternate systems or procedures?
    b. How long can you operate using manual processes or alternate systems when your primary critical systems fail?
    c. What additional staffing requirements are necessary for alternate systems or procedures, if any?
3. How do you respond to widespread power outages?
    a. How do cascading impacts to essential services, critical infrastructure, and other sectors impact your restoration priorities?
    b. How will you continue to provide services to your customers while responding to these incidents?

Module 2: Questions Cont.

4. What information are you sharing internally (e.g., with employees, leadership)?
5. What information are you sharing externally (e.g., with customers, partners)?
6. Describe your organizational processes to respond to the media reports and inquiries.
   a. What pre-scripted messages have been developed for cyber incidents?
   b. What training do your communications personnel receive on cyber terminology?
   c. How would public messaging be coordinated and disseminated during a cyber incident?
   d. How would you work to regain public trust and the trust of your customers following this incident
7. What legal and regulatory notifications are required based on the scenario?
   a. When are notifications made?
   b. Who is responsible for making the notifications?

Module 2: Cont.

Day 18

Your organization is conducting rolling blackouts as staff work to ensure systems are fully operational following the incident. The source of the initial intrusion appears to be an unpatched legacy edge device. Malicious cyber actors exploited a known vulnerability and then used DDoS attacks to evade detection and mask their activity. The threat actors then moved laterally through your system into the OT network to disrupt power generation and distribution.

Module 2 Cont.

1. When would your organization transition to the recovery and post-incident phases?
    a. How is the decision to transition to the recovery phase made?
    b. How does your organization conduct post-incident review?
    c. How are lessons learned/areas for improvement incorporated into process improvement planning (e.g., incident response plans, training)?
2. How do you verify the integrity of your critical systems following a cyber incident?
    a. What actions do you take to mitigate future vulnerabilities?
3. What supply chain challenges would you anticipate when restoring damaged/destroyed equipment?
4. Based on discussion and lessons learned, what changes will you implement to increase the resilience of your organization?

Lesson Learn/Hot Wash

Key Takeaways

- Strengths
- Areas for Improvement
- Action Items
- Something You Learned

Additional Comments

Closing Comments

Cameron Zahn

Outage Management and Compliance Supervisor

Points of Contact

Nicholas M. Dusak
CIP Compliance Officer
City of Denton – Denton Municipal Electric (DME)
Office: (940) 349-7619
Cell: (682) 433-8627

Chad Johnston
Protective Security Advisor-North Texas
Cybersecurity and Infrastructure Security Agency
Integrated Operations Division-Region 6
Cell: (501) 414-1468
Email: Chad.Johnston@cisa.dhs.gov

Joshua Velasquez, MPA
Protective Security Advisor- North Texas District
U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Cell: 202-779-0662
Email: joshua.velasquez@cisa.dhs.gov

END PRESENTATION

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY