

Cybersecurity Wargames for Small Intelligent Transportation Systems Teams

www.its.dot.gov/index.htm

Final Report—May 2024

FHWA-JPO-24-137



U.S. Department of Transportation

Produced by Cambridge Systematics with our teaming partners
U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office
Federal Highway Administration
Office of the Assistant Secretary for Research and Technology
Federal Transit Administration

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-24-137		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Cybersecurity Wargames for Small Intelligent Transportation Systems Teams				5. Report Date May 2024	
				6. Performing Organization Code	
7. Author(s) Marisa C. Ramon, Sabrina E. Mosher				8. Performing Organization Report No. 1.0	
9. Performing Organization Name and Address Southwest Research Institute (SwRI) 6220 Culebra Rd. San Antonio, TX 78227 Under Contract to Cambridge Systematics Inc.				10. Work Unit No. (TRAIIS)	
				11. Contract or Grant No. 693JJ322A000003	
12. Sponsoring Agency Name and Address U.S. Department of Transportation ITS Joint Program Office—HOIT 1200 New Jersey Avenue, SE Washington, DC 20590				13. Type of Report and Period Covered Final Report, May 2024	
				14. Sponsoring Agency Code	
15. Supplementary Notes None					
16. Abstract The United States Department of Homeland Security (DHS) has identified the U.S. transportation system as one of “16 critical infrastructure sectors.” The Intelligent Transportation Systems (ITS) Cybersecurity Program Area was developed in response to this need to protect ITS from cyberattacks. To facilitate that end, this guide was developed to allow State, Local, Tribal, and Territorial (SLTT) agencies to develop and conduct a pilot cybersecurity wargaming exercise that evaluates the cyber readiness of their operations and teaches participants about agency cyber policies and procedures. This guide provides planning steps and example scenarios that SLTT agencies can use to run a cybersecurity wargaming exercise without assistance from external parties.					
17. Keywords Transportation, Cyber Resilience, Cyber Incident			18. Distribution Statement		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 88	22. Price N/A

Table of Contents

1. Executive Summary	1
2. Introduction	3
2.1 Exercise Pilots	3
3. How To Use This Guide.....	5
3.1 Planning an Exercise	5
3.2 Before the Exercise	5
3.3 During Exercise	6
4. State, Local, Tribal, and Territorial Agency Considerations.....	7
4.1 High-Level Goals.....	7
4.2 Resources Planning.....	7
4.2.1 Stakeholders and Participants.....	8
4.2.2 Objectives	8
4.2.3 Cost	8
4.2.4 Facilities	8
4.2.5 Scheduling	9
4.3 Objectives and Desired Outcomes	9
5. Participant(s) and Stakeholders	11
5.1 Participants	11
5.2 Stakeholder Identification	11
6. Conducting Wargame Exercise	13
6.1 “Before” Activities (Pre-Exercise).....	13
6.1.1 Included Materials	13
6.1.2 Additional Materials	13
6.1.3 Participant Roles	14
6.1.4 Scenario Type Selection.....	14
6.2 Scenario Selection Questionnaire	15
6.3 Instructions	19
6.3.1 Gameplay Flow.....	19
6.3.2 General Rules.....	21
6.4 Scenarios	21
6.4.1 Wargame Exercise—Scenario 1	22
6.4.2 Wargame Exercise—Scenario 2.....	27

6.4.3 Wargame Exercise—Scenario 3.....	33
6.4.4 Wargame Exercise—Scenario 4.....	38
6.4.5 Wargame Exercise—Scenario 5.....	44
6.5 “After” Activities (Post-Exercise)	50
6.5.1 Exercise Objectives.....	50
6.5.2 Evaluation Metrics	50
6.5.3 After-Action Report with Improvement Plan	50
7. Conclusion	53
8. References.....	55
9. Supporting Materials.....	57
9.1 Visual Questionnaire Guide.....	58
9.2 Example Scenario Selection	60
9.3 Example Scenario Gameplay	62
9.3.1 Before Gameplay	62
9.3.2 Turn 1	62
9.3.3 Turn 2	62
9.3.4 Turn 3	63
9.3.5 Turn 4	64
9.3.6 Inject Selection	64
9.3.7 Ending	64
9.4 Example Evaluation	65
9.5 Report Templates.....	66
9.5.1 Exercise Evaluation Guide Template.....	66
9.5.2 After-Action Report/Improvement Plan Template.....	69
9.6 Exercise Game Mats	70
9.6.1 Cheat Sheets	70
9.6.2 Gaming Mats for Facilitators.....	72

List of Tables

Table 1. Roles within the exercise team..... 14

Table 2. Scenario questionnaire..... 16

Table 3. Scenario selection table template. 17

Table 4. Scenario modifier values. 18

Table 5. Scenario 1 timed narrative. 22

Table 6. Scenario 1 random narrative injections. 23

Table 7. Scenario 1 narrative ending. 25

Table 8. Scenario 1 evaluation and scoring. 26

Table 9. Scenario 2 timed narrative—default narrative..... 27

Table 10. Scenario 2 timed narrative—alternative narrative. 28

Table 11. Scenario 2 random narrative injections. 28

Table 12. Scenario 2 narrative ending. 31

Table 13. Scenario 2 evaluation and scoring. 32

Table 14. Scenario 3 timed narrative. 33

Table 15. Scenario 3 random narrative injections. 34

Table 16. Scenario 3 narrative ending. 36

Table 17. Scenario 3 evaluation and scoring. 37

Table 18. Scenario 4 timed narrative—default narrative..... 39

Table 19. Scenario 4 timed narrative—alternative narrative. 39

Table 20. Scenario 4 random narrative injections. 40

Table 21. Scenario 4 narrative ending. 42

Table 22. Scenario 4 evaluation and scoring. 43

Table 23. Scenario 5 timed narrative. 45

Table 24. Scenario 5 random narrative injections. 45

Table 25. Scenario 5 narrative ending. 47

Table 26. Scenario 5 evaluation and scoring. 49

Table 27. Example of Scenario 3 evaluation and scoring. 65

Table 28. Quick reference of document section numbers for each scenario..... 72

List of Figures

Figure 1. Flow chart. Exercise flow.	6
Figure 2. Icons. Cybersecurity wargaming exercise resource variables.	8
Figure 3. Infographic. SMART objectives.....	9
Figure 4. Flow chart. Gameplay flow.....	20
Figure 5. Diagram. Example of questionnaire for scenario selection.	58
Figure 6. Diagram. Example of scenario selection and scenario modifier.	59
Figure 7. Example table. Completed questionnaire for scenario selection.....	60
Figure 8. Diagram. Example of completed scenario selection and scenario Modifier.	61
Figure 9. Sample Layout. Template to capture top strengths and weaknesses.	66
Figure 10. Sample Layout. Template to capture observations and notes on objectives.....	67
Figure 11. Sample Layout. Template to record other observations, notes, and recommendations.....	68
Figure 12. Sample Layout. Template for after-action report/Improvement plan.	69
Figure 13. Flow chart. Scenario gameplay.....	71
Figure 14. Diagram. Game facilitator reminders.	72
Figure 15. Representation. Wargame exercise—gameplay mat.	73
Figure 16. Representation. Wargame exercise—timed injects mat.....	74
Figure 17. Representation. Wargame exercise—endings, objectives, and evaluation mat.	75

List of Abbreviations

AAR/IP	After-Action Report/Improvement Plan
ATMS	Advanced Traffic Management System
CCTV	Closed-Circuit Television
CISO	Chief Information Security Officer
CFO	Chief Financial Officer
DHS	Department of Homeland Security
DMS	Dynamic Message Sign
DDOT	The District Department of Transportation
DOT	Department of Transportation
EEG	Exercise Evaluation Guide
FHWA	Federal Highway Administration
IT	Information Technology
ITS	Intelligent Transportation Systems
KDOT	Kansas Department of Transportation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PennDOT	Pennsylvania Department of Transportation
PIO	Public Information Officer
PoC	point of contact
TMC	traffic management center
TTX	Tabletop Exercise
TxDOT	Texas Department of Transportation

SLTT	State, Local, Tribal, and Territorial
SMART	Specific, Measurable, Achievable, Relevant, and Time-bound
UASI	Urban Areas Security Initiative
USDOT	United States Department of Transportation

List of Glossary Terms and Iconography



Injects: Events introduced over the course of the exercise that change or add additional information on the scenario. There are two types of injects.



Timed injects: Occur at a fixed time during the game.



Randomized injects: Each scenario has different randomized injects or action results. Participants randomly select a number between 1 and 20 to resolve whether an action has a positive or negative impact on the scenario narrative. This will be referred to as “roll a D20.” See ***Additional Materials*** (section 6.1.2), for more details.



Variations: All scenarios make some basic assumptions about your organization. Some alternative options within a scenario have been provided in the case the assumption does not fit your organization. If no variation is applicable to your organization, repeat steps 3-5 of the “Scenario Questionnaire” to select a different scenario.



Modifier: This value is determined during scenario selection questionnaire and influences gameplay. It is only used when explicitly stated within the scenario.



Game Clock: A counter of the time as you move through the game. Timed injects occur at a fixed time on the game clock and each turn counts as 10 game minutes. Depending on player actions, additional time may be added.

Game Minute: Units of time in the game will be measured in game minutes to determine progression through a scenario. This is not necessarily the same as real world time. For example, 10 game minutes reflects 10 minutes that have passed for the scenario but may take less than 10 real world minutes of going through the game.



Turn: The period in which participants may take an action in response to an inject. The end of a turn is marked when participants have completed their actions or when the next timed inject occurs. Each turn should take NO MORE than 10 REAL WORLD minutes, and 10 game minutes should be added to the game clock per turn.



Action: The response of a player to an inject during a turn. The action depends on the participant’s role and should be based on how a participant would react to a real incident.



Endings: Potential endings to the scenario based on gameplay. Each scenario has multiple endings. Once participants reach the end of the scenario, the facilitator selects the appropriate ending based on the “Player Action Summarized” options.



Objectives: Specific goals tailored to a given scenario. Player performance should be measured based on how closely players meet the given objectives.

1. Executive Summary

This document presents the Cybersecurity Wargaming Exercise Guide and Supporting Materials (the “Wargaming Exercise Guide”) developed as part of the Federal Highway Administration’s (FHWA) program, “Intelligent Transportation Systems (ITS) Cybersecurity Model for State, Local, Tribal, and Territorial (SLTT) Agencies’ Wargaming Exercises.”

This guide provides all necessary materials for a small group of transportation personnel to conduct a cybersecurity wargaming exercise independently, without assistance from external parties. Agencies may leverage this guide to informally evaluate or improve cybersecurity awareness. Individual exercises can be tailored to match agency policies and goals. While this cybersecurity wargaming exercise can be run by larger agencies to help train personnel on cybersecurity policies, it is best suited for smaller, resources constrained, SLTT agencies operating ITS systems.

Before beginning any cybersecurity wargaming exercise, an SLTT agency should take agency resources into considerations and determine relevant stakeholders. An agency should also establish “why” the exercise is being done and establish overall exercise objectives.

This guide describes how participants should act before, during, and after an exercise.

- **Before an Exercise:**
 - Participants review the purpose, scope, and goals of the exercise, and establish necessary ground rules.
 - This guide provides a questionnaire to assess the current cybersecurity level and select the most applicable cybersecurity wargaming scenario.
 - Participants should review scenario instructions and gameplay flow.
- **During an Exercise:**
 - Participants will play through one of five cybersecurity wargaming scenarios provided in this guide. These scenarios vary in scope and encompass different aspects of transportation operations within a SLTT agency, emphasizing Operational Technologies (OT). Transportation agencies can adapt scenarios to suit organizational needs and structure.
- **After an Exercise:**
 - Participants review actions taken during the exercise and evaluate overall performance.
 - Evaluation criteria is based on the wargame exercise objectives.
 - This guide provides rubrics for evaluating a cybersecurity wargaming exercise. Participants should further summarize results and potential remediation steps in an After-Action Report/Improvement Plan (AAR/IR).

**This guide is a tool for agencies to use when running a cybersecurity wargaming exercise.
It is not intended to be read in one entire sitting.**

2. Introduction

The U.S. Department of Transportation (USDOT) ITS Cybersecurity Program area was developed in response to the urgent need to protect ITS from cyberattacks. Securing transportation's critical assets and infrastructure against cyber threats is a shared responsibility of both the public and private sectors. Executive Order 13800 (issued May 11, 2017) encourages Federal agencies to work with their industries and all entities to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The ITS Cybersecurity Program works with the transportation community to (among other initiatives):

- Identify needs and gaps in cybersecurity vulnerabilities, policies, and response procedures.
- Advance the technical research that adopts or adapts implementation practices from other industries or develops new approaches specific to transportation.
- Create the tools and resources for effectively managing cyber-risk within public transportation systems.
- Provide technology and knowledge transfer to support the transportation workforce in their understanding of cyber issues and mitigations.

This objective of this document is to provide a **Cybersecurity Wargaming Exercise Guide** that is scalable for small to medium sized SLTT transportation agencies. The guide is designed to allow SLTT agencies to run the exercise independently without assistance from external parties.

This guide consists of the following information:

- SLTT Agency Considerations
- Stakeholders and Participants
- Process for Conducting a Wargame Exercise
- Wargame Exercise Evaluation

2.1 Exercise Pilots

To ensure the completeness, effectiveness, and accuracy of this document, several live pilots of the cybersecurity wargaming scenarios presented in this guide were conducted with the five SLTT agencies acknowledged below.

- Kansas Department of Transportation (KDOT)
- Texas Department of Transportation District Office in San Antonio (TxDOT)
- The District Department of Transportation in Washington D.C. (DDOT)
- City of Franklin, Tennessee
- Pennsylvania Department of Transportation (PennDOT)

These stakeholders reflect a variety of transportation agencies based on scale and scope and have greatly contributed to the development of this guide.

3. How To Use This Guide

This guide is not intended to be read in its entirety in a single sitting. It is intended to be used as a tool to guide each step of preparing and running a cybersecurity wargaming exercise.

3.1 Planning an Exercise

There are several considerations an agency must review before beginning a cybersecurity wargaming exercise, such as time, cost, and objectives, which are further discussed in *section 4*. Agencies should also determine relevant participants and stakeholders, which are further discussed in *section 5*.

3.2 Before the Exercise

Participants should prepare relevant materials before gameplay. This document includes several visual guides and cheat sheets participants may find useful. Print these guides in advance and distribute them to the players before beginning a cybersecurity wargaming exercise.

- Scenario Questionnaire
 - Textual Questionnaire (*section 6.2*)
 - Visual Questionnaire (*section 9.1*)
- Gameplay Cheat Sheet (*section 9.6.1*)
- Gameplay Mat (*section 9.6.2*)
- Exercise Evaluation Guide (EEG) Template (*section 9.5.1*)
- Scenario (an individual scenario may be printed after scenario selection) (*section 6.4.1-6.4.5*)

3.3 During Exercise

Each exercise consists of a sequence of steps as shown in *figure 1*. Before beginning gameplay, participants must first designate player roles. They should then take a moment to select the scenario and familiarize themselves with the rules before beginning gameplay.

- Before Activities (*section 6.1*)
 - Designate Roles (*section 6.1.3*)
 - Scenario Selection (*section 6.1.4*)
 - Instructions (*section 6.2*)
- Scenario (*section 6.4.1–6.4.5*)
- Evaluation (*section 6.5*)



Source: FHWA.

Figure 1. Flow chart. Exercise flow.

4. State, Local, Tribal, and Territorial Agency Considerations

Before beginning a cybersecurity wargaming exercise, agency organizers should consider their high-level goals, resources available, and expected exercise participants. Each of these elements directs the planning and execution of the exercise.

4.1 High-Level Goals

The primary goals for the exercise are listed below:

1. Familiarize personnel with agency procedures in a no-fault/no-blame environment.
2. Identify gaps in existing policies and procedures.
3. Strengthen the organization and improve cyber awareness and posture.

Cybersecurity wargaming exercises should help strengthen the organization and improve the cyber awareness of participants. Participants should leave the exercise feeling that they have gained useful experience and knowledge.

When defining the high-level goals, the SLTT agency, stakeholders, and participants should take care to approach the exercise with a no-fault/no-blame attitude. Participants should understand that the process is being examined, not exercise personnel. Putting participants on the defensive will reduce much of the exercise's potential value (and make it harder to find participants for future exercises).

4.2 Resources Planning

Outside of conducting the exercise itself, there are several resource variables the agency must consider. This exercise is intended as an informal exercise among co-workers with limited budget and minimal personnel. Other resource considerations may include facility space and participant time.

The primary resource variables that a SLTT agency must consider prior to running the cybersecurity wargaming exercise are shown in *figure 2*.

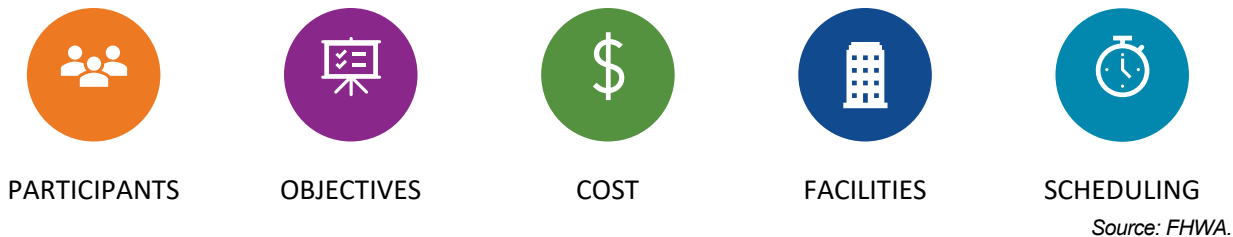


Figure 2. Icons. Cybersecurity wargaming exercise resource variables.

4.2.1 Stakeholders and Participants

Stakeholders will define what the SLTT wants to get out of the exercise, aside from improving their security posture. Because the wargame is designed to educate operations personnel and improve day-to-day operations in a no-fault environment, participants should consist of operations personnel, and high-level officials and agency leadership should **only** be involved for stakeholder buy-in and exercise reporting activities. The number of participants of the exercise may vary. While each exercise can be run by a single participant, having a broad range of participants allows for a more realistic exercise and provides experience to a wider cross-section of groups within the SLTT organization. Coordination will naturally become more challenging as the number of participants grows.

4.2.2 Objectives

Different stakeholders may approach the exercise with different assumptions. Explicitly noting the exercise objectives will help to identify shortfalls during the planning process. See *section 4.3* for additional information on identifying objectives.

4.2.3 Cost

This exercise is modeled as a tabletop exercise, or TTX, meaning it is a discussion-based exercise.¹ As such, it does not require specialized resources or functional components, and can be successfully conducted with little to no funding, exclusive of the stakeholder/participants' time commitment and/or reservation of facilities, if desired.

4.2.4 Facilities

Most organizations will be able to host a successful wargame in their existing facilities. No special facility is required to conduct this exercise. However, exercise planners should consider communication

¹ The DHS/CISA Communications-Specific Tabletop Exercise Methodology contains a wealth of knowledge in planning and conducting tabletop exercises to evaluate communications plans: https://www.cisa.gov/sites/default/files/publications/CommunicationsSpecificTabletopExerciseMethodology_0.pdf.

requirements regarding onsite versus remote participants. Additionally, holding the exercise offsite may help participants to step into their roles more completely (and prevent distractions from routine work).

4.2.5 Scheduling

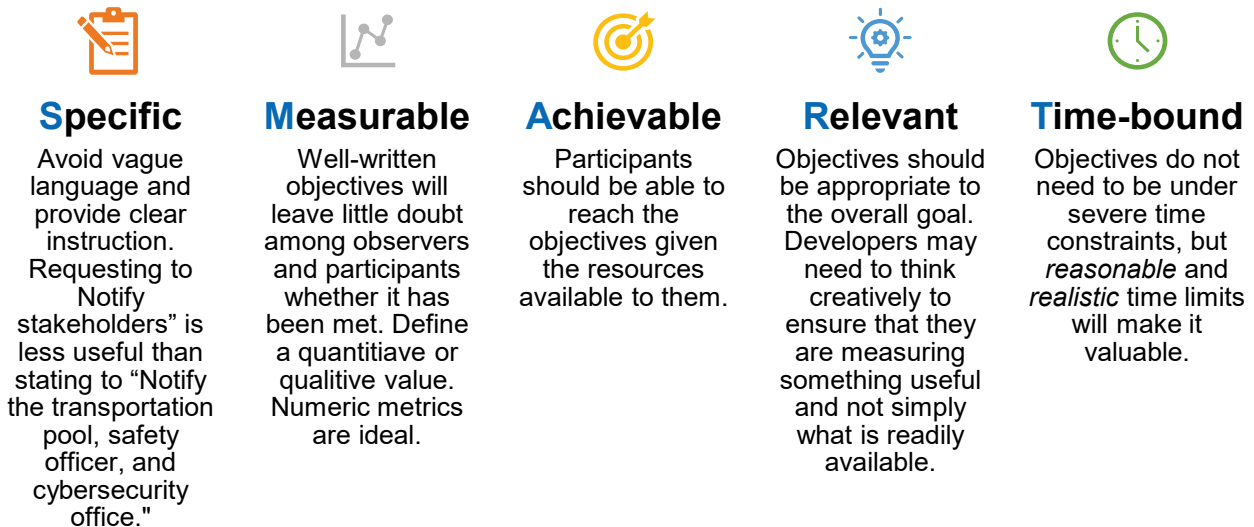
Exercises length may vary based on the number of participant and the level of discussion during game play. A single exercise may take as little as one (1) hour or up to four (4) hours. The longer an exercise is, the more difficult it will be to schedule among participants (and possibly to reserve facilities). Different roles will also include different time commitments; exercise leaders will be coordinating before and after the exercise is conducted. If senior leaders or external stakeholders will be observing the cybersecurity wargaming exercise, their schedules may also be a consideration.

4.3 Objectives and Desired Outcomes

When conducting a cybersecurity wargaming exercise, stakeholders (discussed in *section 5.2*) need to establish the exercise's objectives and desired outcomes. SLTT agencies should decompose the high-level exercise goals, which are general and difficult to measure, into more concrete and measurable tasks. Each exercise in this guide provides specific exercise objectives.

Decomposing the high-level goal into measurable objectives will guide evaluation of participant actions (Note that if there is more than one participant the objectives might not be shared with the other exercise participants in advance, to keep the exercise more realistic.). These objectives should be reevaluated every time an exercise is performed to ensure that they still align with agency needs and overall goals.

Exercise objectives are useful when they conform to the SMART (Specific, Measurable, Achievable, Relevant, and Time-bound) guidelines, as shown in *figure 3*.



Source: FHWA.

Figure 3. Infographic. SMART objectives.

For a half-day cybersecurity wargaming exercise, planners should aim for three strong objectives. More ambitious efforts are possible, but a few strong objectives will be more valuable than many vague, unmeasurable, or unrealistic ones.

Each cybersecurity wargaming exercise in this guide has several associated exercise objectives. Exercise leadership may modify these provided exercise objectives or add additional objectives as desired. As stated in the High Levels Goals section, the exercise should familiarize personnel with agency procedures and to identify gaps in existing procedures. Exercise leadership may further wish to focus on a specific procedure for a given exercise. For example, an exercise might focus on specific communications channels between pertinent organizations. In this case, an example objective might be that every relevant organization is notified at the appropriate time in the exercise.

Two objectives exercise leaders may wish to incorporate into any given exercise are included below:

- **Example Objective 1.** Identify gaps in the cyber incident response manual. Participants should detect an incident, initiate the appropriate response, and inform senior leadership within two hours (simulation time). Any ambiguities or gaps in the response plan will be documented for review.
- **Example Objective 2.** Familiarize SLTT agency personnel with organizational security policies for reporting cyber incidents. Participants should identify a suspected cyberattack within two hours and report the incident to the correct party according to the organization's incident response plan.

5. Participant(s) and Stakeholders

Wargaming exercise participants should consist of those responsible for day-to-day operation of the SLTT's agency's OT assets. The participant(s) is responsible for staging, running, and evaluating the exercise. The number of participants may vary based on the SLTT's stakeholder pool and the scope and objectives of the cybersecurity exercise. The SLTT agency should invite key stakeholders to support the exercise and ensure the exercise meets agency objectives. To achieve the goal of educating operations personnel on cybersecurity policies and procedures, high-level agency officials should **only** be involved for stakeholder buy-in and exercise reporting activities.

5.1 Participants

Participants should be drawn from operations personnel who typically work together. Matching the player's in-game job in the exercise to their real-world role will help to make the exercise more realistic. Additional personnel may be needed based on the exercise goal. Alternatively, putting players in jobs different from their normal jobs (for example, having operators roleplay as Information Technology (IT) technicians, and vice-versa) may help them to gain a larger perspective.



Example **participants** include, but are not limited to:

- Traffic engineers and operators.
- Emergency management personnel.
- IT technicians responsible for operational technology (OT) assets and network.
- Signals and ITS field technicians.
- Personnel responsible for day-to-day OT operations, including third-party contractors.

5.2 Stakeholder Identification

Although this wargame is directed at operational staff, key stakeholders should be invited to support various phases of the cybersecurity wargaming exercise. These stakeholders should come from the SLTT and include all parties relevant for a cybersecurity incident. A SLTT agency may have many relevant stakeholders, and each of these stakeholders can play a role in setting wargame objectives. A larger group of stakeholders involved maximizes the return on the investment of conducting this exercise.

It is important to note that **high-level officials and department of transportation (DOT) leadership should be limited to stakeholder buy-in and exercise reporting activities**. These exercises are designed to educate operations personnel on their day-do-day activities in a no-fault/no-blame environment. Operations personnel may feel intimidated by high-level officials or defer to their authority. The results of the exercise in this case would then be inaccurate.

Example **stakeholders** include, but are not limited to:

- High-level SLTT Government officials and leadership:
 - Director
 - Public Information Officer (PIO)
 - Chief Financial Officer (CFO)
 - Program Coordinator of Training & Exercise
 - Tribal Governor, Chief, Chair, or President
- Cybersecurity personnel:
 - Chief Information Officer (CIO) and/or Chief Information Security Officer (CISO)
 - Chief Technology Officer (CTO)
 - Homeland Security Advisor
 - Cybersecurity Manager
 - Cybersecurity Analyst
 - Privacy Officer
 - Urban Areas Security Initiative (UASI) Program Manager
 - Urban-area security directors

6. Conducting Wargame Exercise

The following sections describe the process for conducting a cybersecurity wargaming exercise. Before beginning an exercise, participants must select a scenario and review gameplay instructions. Once participants have completed an exercise, they should evaluate gameplay results.

6.1 “Before” Activities (Pre-Exercise)

Before beginning the cybersecurity wargaming exercise, the participants should coordinate to determine exercise roles and establish a date, time, and location for the event. All participants should be briefed on the purpose, scope, and goals of the cybersecurity wargaming scenario. Any pre-reading materials should also be provided at this stage. Remind participants that this is a “no fault/no blame” environment and they must respond to the exercise as honestly and realistically as possible.

6.1.1 Included Materials

Several optional gameplay tools are provided in this guide to facilitate gameplay. Print these materials before gameplay.

- Scenario Questionnaire: A guide for scenario selection. (*section 6.2*)
- Scenario Gameplay Cheat Sheet: This can be distributed among the players to help players follow game flow and give reference instructions. (*section 9.6.1*)
- Scenario Gameplay Game Mat: Optionally used during scenario gameplay to assist in keeping track of game progress for any scenario. (*section 9.6.2*)

6.1.2 Additional Materials

Several materials not provided in this guide are necessary for the exercise.

- Notetaking material: this is anything that could be used for notetaking, such as a laptop or paper and pen.
- A random number generator from 1-20:
 - Participants can use a random number generator (min: 1, max: 20) from a phone application or website (e.g., Google’s virtual 20-sided dice: <https://www.google.com/search?q=d20> or a random number generator: <https://www.google.com/search?q=random+number+generator>).
 - Optionally, participants may use a physical 20-sided dice, or “D20” as its commonly referred to.

6.1.3 Participant Roles

There are four roles participants may take on as described in *table 1*. Participants may take on multiple roles. All participants should be players. At least one notetaker and one clock keeper should be designated before gameplay. The role of facilitator is optional.



Table 1. Roles within the exercise team.

Role	Description
Player	Analyzes the challenges presented in the exercise and propose timely solutions. Players(s) are being evaluated on their performance in the exercise to aid in identifying gaps in policy, procedures, or staff training.
Notetaker (can be a player)	Observe exercise and record player activity. The notetaker keeps track of scenario selection and, at the end of the exercise, uses notes to help the group evaluate their performance and generate action items based on and exercise goals and objects. A player can take on the role as a note taker in addition to playing in the exercise.
Timekeeper (can be a player)	Keeps track of the game clock (measured in game minutes) during the exercise. A player can take on this role as a timekeeper in addition to playing in the exercise.
Facilitator (optional)	Optional role intended to lead players through the exercise by facilitating discussion and deciding which stage of the game the group is at. Note: A more experienced team member is appropriate here, although a team member with experience at tabletop exercises would be a good fit. It is imperative that facilitators do their best to act realistically and avoid leveraging their knowledge of the exercise to get a better result. They will also have to decide how much information to provide to other participants to keep the exercise moving without providing an unrealistic amount of inside information.

Source: FHWA.

6.1.4 Scenario Type Selection

After participants have been given roles, it is time to select a scenario. Several scenarios are provided later in this document. To select which scenario to run, participants should perform the *Scenario Selection Questionnaire (section 6.2)*. The scores from the questionnaire will also determine a “modifier” that will be used to influence gameplay.



As players become familiar with the scenarios, details can be changed to focus on the desired overall exercise objectives. SLTT agencies can also develop their own scenarios using the guidance and examples provided in this document. The scenarios should be plausible; incorporating real-world events or threats will provide a more realistic experience and improve participant learning.

6.2 Scenario Selection Questionnaire

This questionnaire can be used to find a scenario to select for cybersecurity wargames based on your organization's cybersecurity incident response plan. If you do not have one, congratulations, you have identified your first action item. In this case, complete the questionnaire based on the procedures you would normally follow. Participants will complete the Scenario Questionnaire in *table 2* to develop a **Scenario Sequence Set** that will be used to build the Scenario Selection Table (*table 3*). This table will be used to randomly select a scenario and assign a modifier used during gameplay.

Agencies may also choose to use the results of the questionnaire of a baseline indicator of potential areas of improvement, but the questionnaire itself should not be taken as an overall evaluation. A visual guide on completing the questionnaire is provided in the **Visual Questionnaire Guide** (*section 9.1*). An example scenario selection questionnaire can also be found in **Example Scenario Selection** (*section 9.2*).

1. As a group, read each question in the "Question" column in *table 2* and select the answer in "Scoring" column that is most applicable to your organization. For the selected answer, record the associated **Scenario Sequence Set** in the applicable column.
 - If the group is unsure which answer to pick, select the least secure option (the one with the **longest** scenario number sequence set).
 - Participants should arrive at a consensus agreement on the question answers before moving on to step 2.
 - These questions apply to Operational Technologies and field networks.

Table 2. Scenario questionnaire.

#	Question	Scoring	Scenario Sequence Set
#1	Does your organization have a written policy on password management of field devices? What is the policy?	<ul style="list-style-type: none"> a. No policy on password management: Sequence Set = 5,5,1 b. Policy allows password reuse and/or sharing across devices, but does not allow default passwords: Sequence Set = 5,5 c. Policy does not allow password reuse and/or sharing across devices and does not allow default passwords: Sequence Set = 5 	
#2	Does your organization manage Bluetooth devices (i.e., pedestrian crosswalks)? If so, are there any security policies for protecting these devices?	<ul style="list-style-type: none"> a. The organization manages Bluetooth devices, but there are no validation or encryption policies for communication with devices: Sequence Set = 2,2,2 b. The organization manages Bluetooth devices and does have validation and encryption policies for communication with such devices: Sequence Set = 2,2 c. The organization does not manage Bluetooth devices: Sequence Set = 1 	
#3	Does your organization have policies for protecting against physical access of field devices? Does your organization perform regular backups of operations data?	<ul style="list-style-type: none"> a. If neither is done: Sequence Set = 3,1,1 b. If one is done: Sequence Set = 1,3 c. If both are done: Sequence Set = 1 	
#4	Does your organization secure network communication with field devices?	<ul style="list-style-type: none"> a. There's no known network security policy: Sequence Set = 3,3,5 b. The field device network is segmented from the IT network: Sequence Set = 3,3 c. The field device network is segmented from the IT network, and network traffic is encrypted: Sequence Set = 3 	
#5	Does your organization keep all its services on-site (i.e., no external or third-party service providers)? If not, what is the procedure if there are any issues with these external services?	<ul style="list-style-type: none"> a. A large portion of services are off-site, and there is no process for reporting issues: Sequence Set = 4,4,4 b. There are some off-site services, but there's a policy in place for reporting issues: Sequence Set = 4,4 c. There are no off-site services: Sequence Set = 5 	

Source: FHWA.

2. Populate the Scenario Selection Table (*table 3*) with the **Sequence Sets** determined in the previous step by deconstructing each set of number(s), using the “,” into each row in *table 3* below.

For example: If the answer to the first question was “a. No policy on password management,” then the **Scenario Sequence Set** score will be “5,5,3.” Write “5” in row 1, “5” in row 2, and “3” in row 3. For a more in-depth example, please refer to the **Example Scenario Selection** (*section 9.2*).

Table 3. Scenario selection table template.

Row	Scenario Number
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

Source: FHWA.

3. Randomly select a “Row” from the table filled in the previous step using a random number generator between 1 and X, where X is the number of entries in the table. Use the result to select a “Row.” The corresponding entry in the “Scenario Number” column is the exercise **Scenario Number** and will later designate the scenario selected for the exercise gameplay.
- For example, if there are 11 rows, the X=11. Select a random number between 1 and 11. If the result is 5, select the entry with 5 in the “Row” column. If the corresponding value in the “Scenario Number” column is 3, then the corresponding scenario exercise to play will be Scenario 3.
 - There are several websites and phone applications that can be used as a random number generator. (e.g., Google’s virtual D20: <https://www.google.com/search?q=d20> or a random number generator: <https://www.google.com/search?q=random+number+generator>).

4. Count the number of entries in the “Scenario Number” column in *table 4* that have the same value as the randomly selected **Scenario Number** from Step 3.
 - For example, if your **Scenario Number** is 3 and 3 appears twice in the table, your Scenario Number Count is 2.

Table 4. Scenario modifier values.

Scenario Number Count	Scenario Modifier
1	+3
2	+2
3	+1
4	+0

Source: FHWA.

5. Use the Scenario Number Count in the previous step to find the corresponding entry in the “Scenario Number Count” column in *table 4*. The number in the corresponding “Scenario Modifier” column is your **Modifier**. This **Modifier** is used during the game to adjust the scenario’s difficulty. Only use the **Modifier** as specified in the scenario.
 - For example, if your Scenario Number Count is 2, then your Scenario Modifier will be +2. This is the modifier you will apply throughout the exercise as directed.

Using the *Scenario Number* from Step 3, select the corresponding exercise scenario and begin gameplay. Record your *Modifier* and use it as specified explicitly within the scenario.

Note

Several scenarios have different assumptions or variations based on organizational structure.





If you find that none of the assumptions are applicable to your organization, repeat steps 3-5 above.

6.3 Instructions

Participants should review the instructions for a cybersecurity wargaming exercise before beginning gameplay. The instructions cover general gameplay flow and rules. For terminology definitions, see the Glossary in the table of contents. Participants can find an example of scenario gameplay in **Example Scenario Gameplay** (section 9.3).

6.3.1 Gameplay Flow

The basic flow of the exercise is shown in *figure 4* and is as follows:

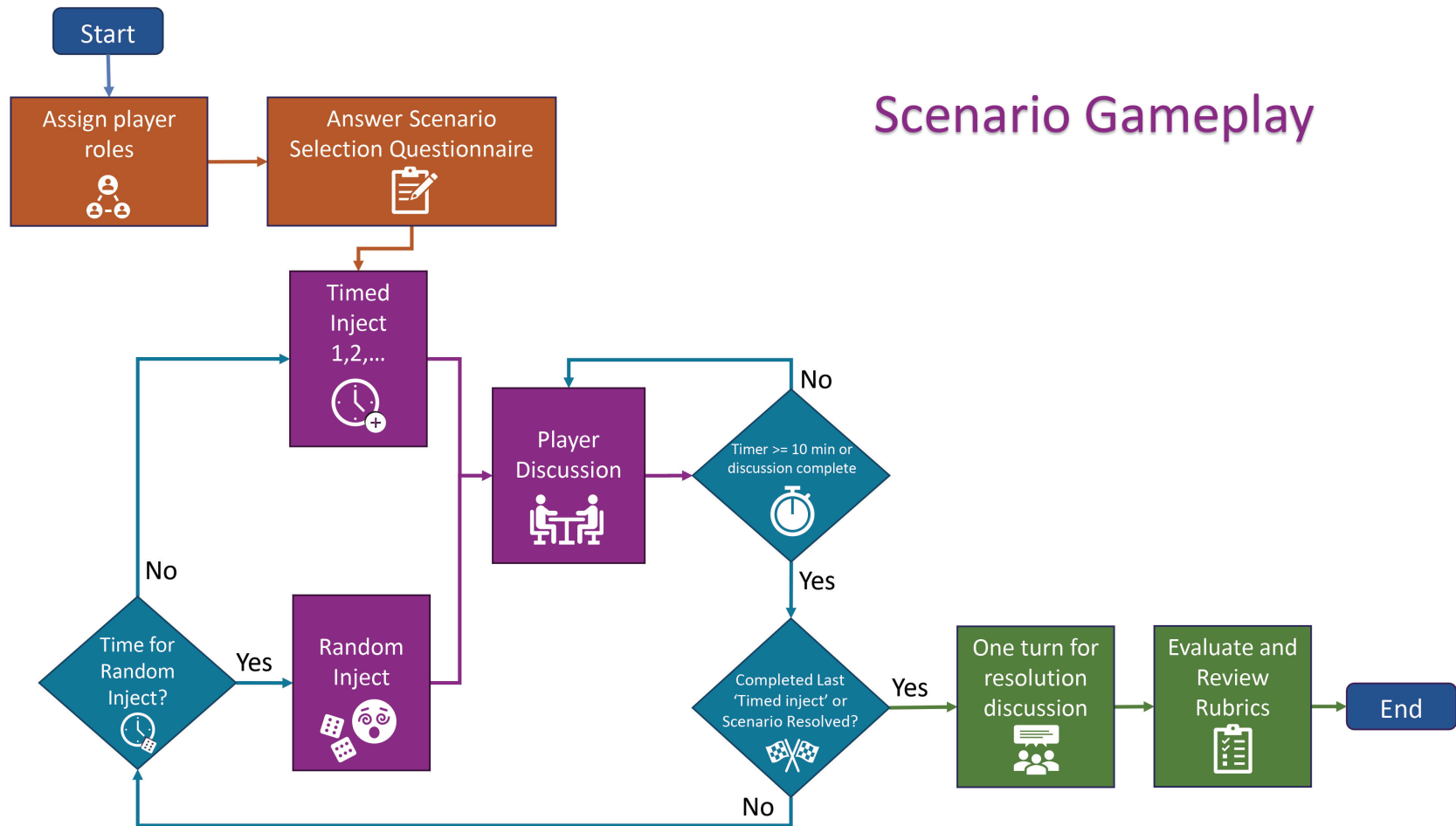
1. Participants begin by reading a timed inject from the established scenario narrative, starting a new turn. The inject is determined by gameplay and the current value of the game clock. 
2. One turn of play begins. Participants take actions according to their role during the turn. **Each participant should take an action or specify that they will take no action.** 
 - A turn should take no longer than 10 real world minutes.
 - Increase the counter for the game clock by 10 game minutes at the end of the turn.
3. If the game clock indicates that a timed inject is necessary (at 50 game minutes or 90 game minutes), go to step one. If players have hit the end of game time (game clock is 120 minutes), move on to step 6. Otherwise, proceed to step 4.
4. Players must determine the appropriate randomized inject. This is done by looking at the list of randomized injects under the “player action” column to find the action that closest matches player choices. Then read the “resulting narrative” column.
 - **Note:** Randomized injects may require the roll of a D20 (a random number between 1-20). If specified, add the modifier to the result to determine your “resulting narrative” (ex: modifier of 3 and roll of 8 gives a result of 3+8=11). 
 - **Note:** Some randomized injects affect the game clock. Make sure to update the clock as specified in the inject.
5. If participants cannot determine an appropriate randomized inject and feel they have fully resolved the scenario, then let there be one more turn of play. Afterwards move on to the exercise ending in step 6.
6. Once players have completed play, they should review the different possible endings. Based on player actions, they should arrive at a specific ending. 

Note

If the team is experienced and find that none of the random injects apply, players or facilitators may wish to create new injects.

Review the exercise evaluation. A description of the exercise evaluation is provided in “After” Activities (Post-Exercise) (section 6.5).

Scenario Gameplay



Source: FHWA.

Figure 4. Flow chart. Gameplay flow.

6.3.2 General Rules

Participants should remember these general rules during gameplay:

- Players must be careful to respond to the exercise as honestly and realistically as possible. Attempting to answer in a way different than you normally would to get the “best” outcome will be of no benefit. This ensures that participants gain experience from the exercise and any gaps in current policies and procedures are revealed.
- There may be multiple solutions to the scenario.
- **This is a “no fault/no blame” environment;** all players should provide their viewpoints without negative repercussions.
- Assume that only known existing organization assets can be used during the scenario.
- Only players can contribute to discussion during the cybersecurity wargaming exercise.
- There are no “trick questions,” and events are presented at face value.

During the exercise, notetakers should be recording participant actions and responses to scenario injects. Notetakers should particularly watch for the following items or actions:

- Policies, procedures, or other documents referenced.
- Technical gaps in responses to questions, or questions left unanswered.
- Use of organizational resources, incident response plans, or processes.
- References to interdepartmental resources.
- Escalations to leadership. When players escalate to leadership and why.

6.4 Scenarios

This guide provides five different wargame scenarios that cover different attack vectors to a SLTT transportation agency. Each scenario consists of a combination of timed narrative injections and random narrative injections based on participant actions. Scenario endings are determined based on player actions during gameplay. Each scenario also contains specific exercise objectives and a specific exercise evaluation rubric.

The participants should include operators and relevant IT and maintenance staff. The jobs and actions of players should reflect on existing jobs in the agency. Players should not take on positions that do not exist within their agency.

A game mat and cheat sheet are included in this guide (*section 9.6*) to guide scenario gameplay. If players want to use the game mat, now is the time to print out the scenario and arrange the injects, endings, and evaluation on the mat.

Participants can find an example of scenario gameplay in ***Example Scenario Gameplay*** (*section 9.3*).

6.4.1 Wargame Exercise—Scenario 1

Time to complete exercise successfully: 120 game minutes

Scenario Selection Questionnaire Modifier Value:

6.4.1.1 Variations

There are no variations for this scenario. Assume different types of devices are affected. Example devices for Inject #1 are listed below:

- Dynamic Message Signs (DMS)
- Closed-Circuit Television (CCTV) Camera
- Traffic Signal
- Traffic Sensor
- Weather Sensor

6.4.1.2 Timed Narrative

Table 5. Scenario 1 timed narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	Operations personnel in a traffic management center (TMC) notice that several devices are showing offline.
Inject 2 [50 game minutes]	Devices along a large section of roadway are no longer functioning. These devices appear to be in a similar region.
Inject 3 [90 game minutes]	All devices are now showing offline.

Source: FHWA.

6.4.1.3 Random Narrative Injections

Select a randomized inject after players have taken their turn based on the “Player Action” column. Then read the “Resulting Narrative.”

Table 6. Scenario 1 random narrative injections.

Random Inject No.	Player Action	Resulting Narrative
#1	Players wait to see if something changes naturally. Add 10 game minutes to game clock.	No change.
#2	Players analyze which devices are showing offline.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 15: Players recognize that the devices showing offline are in the same physical area. The devices are logically connected within the field device network (tied to a common server, common network switch, or same VLAN). <input type="checkbox"/> 8-15: Players recognize that the devices showing offline are in the same physical area. <input type="checkbox"/> < 8: Players do not notice anything. <p>What do you do now?</p>
#3	Players attempt to troubleshoot using the ATMs system (ATMS) or vender software.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 10: The software appears to be functioning properly. Logs indicate network errors attempting to communicate with the offline devices. <input type="checkbox"/> <= 10: Players do not notice anything. <p>What do you do now?</p>
#4	Players investigate recent power outages.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 13: There is a power outage in the area, but investigation finds that the offline devices should not be affected by the outage. <input type="checkbox"/> 7-13: There was a recent power outage in the area. <input type="checkbox"/> < 7: There was a recent power outage in the area. Add 10 game minutes to game clock. <p>What do you do now?</p>

Table 6. Scenario 1 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#5	Players attempt to consult IT support to diagnose network. Add 10 game minutes times modifier to game clock.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 13: IT discovers someone has launched a cyberattack via physical access to a device, causing a network outage. IT quarantines the attack so it cannot spread and finds that the attack comes from a specific traffic box on the roadway. <input type="checkbox"/> 7-13: IT discovers a network problem but cannot narrow down the cause. IT brings down the entire network. <input type="checkbox"/> < 13: Network IT support fails to diagnose any issues and will continue investigating. <p>What do you do now?</p>
#6	Players ask repair crew to check devices that were offline at start of scenario. Add 10 minutes to game clock.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 17: The repair crew comes across two attackers who are accessing the network through a switch in a weatherproof cabinet they have forced open. The attackers flee when they are discovered. Repair crews notice an unusual device in the cabinet. <input type="checkbox"/> 10-17: The repair crew finds that the traffic cabinet has been forced open and notice an unusual device in the cabinet. <input type="checkbox"/> < 10: The repair crew reports that the cabinet has been forced open. Add 10 game minutes to game clock. <p>Play for 1-2 more turns before ending the scenario.</p>
#7	Road crews and players consult IT about the strange device in the cabinet.	<p>IT gives detailed instructions on how to remove the device. After the device is removed, devices appear to be functioning properly again. IT looks closely at the device and determines that it has been used to access the device network.</p> <p>Play for 1-2 more turns before ending the scenario.</p>
#8	Road crews attempt to remove the strange box in the network cabinet.	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> >= 18: Road crews successfully remove the box from the cabinet. Devices appear to be functioning properly again. <input type="checkbox"/> < 18: Road crews remove the box from the cabinet. Suddenly the entire device network shuts down. <p>Play for 1-2 more turns before ending the scenario.</p>
#9	Players consult with IT on the contents of the traffic cabinet.	<p>IT notices a strange device in the traffic cabinet. Add 10 minutes to game time and proceed to Random Inject #7.</p>

Source: FHWA.

6.4.1.4 Narrative Ending

Once players have completed gameplay, allow one turn for any post-scenario player-actions. Then review the player actions during gameplay and select the appropriate ending based on the “Player Action Summarized” column. Read the end of the scenario in the corresponding “Scenario Ending” column.

Table 7. Scenario 1 narrative ending.

Ending No.	Player Action Summarized	Scenario Ending
Ending #1	Players run out of time.	The attacker brings down the entire device network. The TMC experiences several days of downtime.
Ending #2	Players escalate to IT but do not send road crews to investigate.	IT prevents the attack from spreading but is unable to fix the root cause of the incident for several days. Devices remain offline for several days.
Ending #3	Players ask road crews to verify device status but do not consult with IT. Players do not perform an after-action report.	Field technicians confirm that the cabinet was broken into and begin effecting repairs. Because IT was not consulted, the attacker may still have access to the network. The TMC fails to adequately prevent similar attacks in the future.
Ending #4	Players ask road crews to verify device status and properly escalate to IT. Players do not perform an after-action report.	Field technicians and IT jointly remove the malware from the network, and the TMC resumes normal operations. Without an after-action report, the TMC fails to adequately prevent similar attacks in the future.
Ending #5	Players ask road crews to verify device status and properly escalate to IT. Players perform an after-action report.	Field technicians and IT jointly remove the malware from the network, and the TMC resumes normal operations. All parties collaborate on an after-action report, capturing lessons learned and reducing risk in the future.

Source: FHWA.

6.4.1.5 Scenario-Specific Objectives

Now that the scenario has concluded, review the following scenario objectives, and discuss how player actions met or failed to meet them:

1. Operations personnel should be aware of incident response plan policy regarding network outages. Players should be able to diagnose a network outage and identify it as a potential cyberattack. Players should properly escalate to IT support.
2. Personnel should be familiar with procedures regarding attacks on physical traffic cabinets in the case where a cabinet was forced open and unknown hardware was installed.
3. Staff should be aware of incident response plan policy regarding after action reports and lessons learned meetings. Players should be able to identify what changes could be made to prevent the issue from occurring again or develop mechanisms to ensure proper escalation.

6.4.1.6 Evaluation and Scoring

Select the appropriate checklist items and add the score modifiers to establish the ending score.

Table 8. Scenario 1 evaluation and scoring.

Checklist Item	Score Modifier
Ending 1	-30
Ending 2	-10
Ending 3	-10
Ending 4	+15
Ending 5	+20
Positive ending at least 30 game minutes before the scenario time limit.	+10
Players identify the nature of the cyber incident.	+5
Players refer to incident response plan for procedures in responding to the cyber incident.	+15
Players escalate the cyber incident to a relevant point of contact (PoC).	+5
Players attempt to mitigate the damage of the cyber incident.	+5
Players follow scenario closeout procedures according to incident response plan.	+5
Players attempt to investigate the device network.	+10
Players attempt to diagnose the issue using existing software.	+5
Players recognize that the issue might be due to physical access and send road crews to investigate.	+10
Players consult with IT while repairing the traffic cabinet.	+10

Source: FHWA.

Total Score:

6.4.2 Wargame Exercise—Scenario 2

Time to complete exercise successfully: 120 game minutes

Scenario Selection Questionnaire Modifier Value:

6.4.2.1 Variations

This scenario assumes that the agency's traffic management center (TMC) manages Bluetooth pedestrian crosswalks.

Alternative 1

The TMC supports Bluetooth traffic sensors.

1. Use the Alternative Timed Narrative instead of the Default Timed Narrative.
2. Replace "pedestrian crossing" with "traffic sensor" throughout the scenario.

Alternative 2

The TMC supports other Bluetooth devices. There should be multiple of these Bluetooth devices.

1. Use the Alternative Timed Narrative instead of the Default Timed Narrative. Replace "traffic sensor" with the appropriate device.
2. Replace "pedestrian crossing" with the appropriate device name throughout the scenario.

6.4.2.2 Timed Narrative

Table 9. Scenario 2 timed narrative—default narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	The TMC receives a phone call saying that the traffic signals in an intersection with crosswalks are not working.
Inject 2 [50 game minutes]	Monitoring the failed the device, operations personnel notice that the traffic signal is not working again. The TMC starts receiving calls about other signals along the same street failing. They are starting to flash. Personnel note that these signals also have pedestrian crosswalks.
Inject 3 [90 game minutes]	All traffic signals are in flash.

Source: FHWA.

Table 10. Scenario 2 timed narrative—alternative narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	TMC operations personnel notice a Bluetooth traffic sensor is showing in an error state.
Inject 2 [50 game minutes]	Monitoring the failed the device, operations personnel notice that the traffic sensor is not working again. Other similar sensors along the same roadway start failing.
Inject 3 [90 game minutes]	All traffic sensors are entering an error state and other devices in the network are starting to fail.

Source: FHWA.

6.4.2.3 Random Narrative Injections

Select a randomized inject after players have taken their turn based on the “Player Action” column. Then read the “Resulting Narrative.”

Table 11. Scenario 2 random narrative injections.

Random Inject No.	Player Action	Resulting Narrative
#1	Players examine the faulty device using cameras.	Camera images verifies the issue. What do you do now?
#2	Players verify the issue in the ATMS or vender software.	Roll a D20 and add the modifier to the result: <ul style="list-style-type: none"> <input type="checkbox"/> > 10: The software reports the correct device status, but a cursory look at the logs indicates the status was not changed manually. <input type="checkbox"/> <= 10: The software reports the correct device status, but personnel cannot identify if the status was changed by the system. Players can look further and device logs if they choose. What do you do now?
#3	After reviewing ATMS or vender software, players take a closer look at device logs and communication. If modifier is +1 or less, add 10 game minutes to the game clock.	The logs indicate that the issue has been caused by a local Bluetooth pedestrian crossing device changing the traffic signal. <i>If using variation 1 or 2:</i> The logs indicate that the device status was changed by a local Bluetooth connection.

Table 11. Scenario 2 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#4	Players attempt to change the signal timing using the software <i>before Inject #2</i> .	The signal timing updates and appears to be functioning properly. Before long, however, the traffic sensor is no longer changing again. Add 10 game minutes to the game clock. What do you do now?
#5	Players attempt to reset the device status remotely using the software <i>before Inject #2</i>	The device comes online and appears to be working properly. Before long, however, the device is in an error state again. Add 10 game minutes to the game clock. What do you do now?
#6	Players contact the traffic signal vender about the device failure.	Roll a D20 and add the modifier to the result: <input type="checkbox"/> ≥ 10 : Add 10 game minutes to the game clock. <input type="checkbox"/> < 10 : Add 20 game minutes to the game clock. The vender reports that the hardware is not responsible for the failure. The issue has been caused by a local Bluetooth pedestrian crossing device changing the traffic signal. <i>If using variation 1 or 2:</i> The vender reports that the hardware is not responsible for the failure. The device status was changed by a local Bluetooth connection.
#7	Players send field crews to investigate the issue and reboot the device. Add 10 game minutes to the game clock.	Before <i>Timed Inject #2</i> : The device appears to be working again temporarily before it starts malfunctioning again. What do you do now? Add 10 game minutes to the game clock. After <i>Timed Inject #2</i> : All the devices appear to be working again temporarily before they all start malfunctioning again. What do you do now? Add 10 game minutes to the game clock. After <i>Timed Inject #3</i> : Players reboot the device. Nothing happens. What do you do now?

Table 11. Scenario 2 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#8	<p>Players consult IT to diagnose network issues.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Before <i>Timed Inject #2</i>: IT does not notice anything.</p> <p>After <i>Timed Inject #2</i>: There is a significant spike in network activity. Based on historical activity, the spike is abnormal. IT identifies an attack on the field device network and quarantines it. Devices that were affected were disconnected and field crews must manually reconfigure. What do you do now? Play for 1-2 more turns before ending the scenario.</p> <p>After <i>Timed Inject #3</i>: IT sees that the field device network has been flooded and shuts down the network. Personnel must send field crew to manually reconfigure all devices. What do you do now? Play for 1-2 more turns before ending the scenario.</p>
#9	<p>After escalating the network issue to IT, players perform an after-action report.</p>	<p>Investigation finds that the device was using default passwords, allowing the attacker to easily access it and thus access the network. Personnel review the passwords of all devices managed by the TMC to prevent similar attacks in future.</p>

Source: FHWA.

6.4.2.4 Narrative Ending

Once players have completed gameplay, allow one turn for any post-scenario player-actions. Then review the player actions during gameplay and select the appropriate ending based on the “Player Action Summarized” column. Read the end of the scenario in the corresponding “Scenario Ending” column.

Table 12. Scenario 2 narrative ending.

Ending No.	Player Action Summarized	Scenario Ending
Ending #1	Players do nothing.	The attacker remotely connected to the Bluetooth pedestrian crossing device and successfully flooded the network. IT shuts down the entire network, and field crews spend weeks manually fixing devices.
Ending #2	Players update the signal timings or device status but do nothing else.	Because players had fixed the initial issue with the Bluetooth pedestrian crossing device, IT is able to identify the attack more quickly, however the attacker was still able to infiltrate to flood the network. Field crews spend weeks manually fixing affected devices.
Ending #3	Players update the signal timings or device status and alert IT to an issue but do not perform an after-action report.	The attacker remotely connected to the Bluetooth pedestrian crossing and attempted to flood the network. Fortunately, IT identifies the attacker quickly and quarantines the attack. Because no after-action report was performed, the system remains vulnerable to similar attacks in the future.
Ending #4	Players fix the device, alert IT of the issue, and perform an after-action report.	The attacker remotely connected to the Bluetooth pedestrian crossing and attempted to flood the network. Fortunately, IT identifies the attacker before he can and quarantines the attack. The after-action report identifies a password issue with the devices that allowed the attacker to infiltrate the system, and personnel verify that each device managed by the TMC has a unique password to prevent similar attacks in the future.

Source: FHWA.

6.4.2.5 Scenario-Specific Objectives

Now that the scenario has concluded, review the following scenario objectives, and discuss how player actions met or failed to meet them:

1. Players should be aware of vulnerabilities in Bluetooth devices and familiar with organizational procedures to respond to and mitigate an attack via Bluetooth. Players should be familiar with policies for reporting suspected incidents.
2. Staff should be aware of incident response plan policy regarding after action reports and lessons learned meetings. Players should be able to identify what changes could be made to prevent the issue from occurring again or develop mechanisms to ensure proper escalation.

6.4.2.6 Evaluation and Scoring

Select the appropriate checklist items and add the score modifiers to establish the ending score.

Table 13. Scenario 2 evaluation and scoring.

Checklist Item	Score Modifier
Ending 1	-25
Ending 2	-30
Ending 3	+15
Ending 4	+20
Positive ending at least 30 game minutes before the scenario time limit.	+10
Players identify the nature of the cyber incident.	+5
Players refer to incident response plan for procedures in responding to the cyber incident.	+15
Players escalate the cyber incident to a relevant PoC.	+5
Players attempt to mitigate the damage of the cyber incident.	+5
Players follow scenario closeout procedures according to incident response plan.	+5
Players attempt to diagnose the issue remotely.	+10
Players verify the issue is not in traffic management or vendor software	+5
Players attempt to fix issues with signal timing and device status.	+5
Players escalate the issue to IT as a potential network issue.	+10
Players perform an after-action report	+5

Source: FHWA.

Total Score:

6.4.3 Wargame Exercise—Scenario 3

Time to complete exercise successfully: 120 game minutes

Scenario Selection Questionnaire Modifier Value:

6.4.3.1 Variations

There are no variations for this scenario. Events that occur can apply to any device managed by a traffic management center (TMC), but players may wish to select a specific device. Example devices for Inject #1 are listed below:

- Dynamic Message Signs (DMS)
- Closed-Circuit Television (CCTV) Camera
- Traffic Signal
- Traffic Sensor
- Weather Sensor

6.4.3.2 Timed Narrative

Table 14. Scenario 3 timed narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	While most devices seem to be operating normally, communication with several devices of the same type seems to be slower than normal (i.e., timeouts, waiting for a response).
Inject 2 [50 game minutes]	Communication with all devices of the same type has slowed almost to a halt. Personnel must wait several minutes before getting a response from any device.
Inject 3 [90 game minutes]	Several systems across the network are down. Personnel are unable to use the network for any reason.

Source: FHWA.

6.4.3.3 Random Narrative Injections

Select a randomized inject after players have taken their turn based on the “Player Action” column. Then read the “Resulting Narrative.”

Table 15. Scenario 3 random narrative injections.

Random Inject No.	Player Action	Resulting Narrative
#1	Players attempt to view camera footage or retrieve camera snapshots to verify the issue.	Players are unable to view camera footage, and requests for snapshots take several minutes to receive. What do you do now?
#2	Players attempt to determine if the slowness is caused by the software. If modifier is +1 or less, add 10 game minutes to the game clock.	Roll a D20 and add the modifier to the result: <input type="checkbox"/> > 10: The slowness is not caused by in the software. <input type="checkbox"/> <= 10: It is uncertain whether the slowness was caused by the software. What do you do now?
#3	If players have an ATMS system, the players attempt to instead use vender software to communicate with devices.	Communication to devices is slow using the vender software. What do you do now?
#4	Players reach out to the ATMS provider to narrow down the source of the slowness. Add 10 game minutes to game clock.	The ATMS provider indicates that the slowness is not caused by the ATMS software. What do you do now?
#5	Players reach out to hardware venders to determine what could have caused the slowness. Add 10 game minutes to game clock.	Roll a D20 and add the modifier to the result: <input type="checkbox"/> > 10: The venders indicate that the slowness is not caused by devices. <input type="checkbox"/> <= 10: The venders are unable to determine if the devices themselves are causing the slowness without further investigation. What do you do now?
#6	Players attempt other workarounds to communicate with devices.	There is no improvement in device communication. What do you do now?
#7	Players contact other TMCs or districts to see if they are seeing similar issues.	Nobody else is experiencing this issue. What do you do now?

Table 15. Scenario 3 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#8	Players reboot the system before <i>Timed Inject #3</i> .	<p>Roll a D20:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 15: After the reboot, the system appears to be functioning normally. Add 10 game minutes to game clock. The system begins to slow down again. <input type="checkbox"/> 5-15: Nothing changes. Add 10 game minutes to the game clock. <input type="checkbox"/> < 5: Skip to <i>Timed Inject #3</i>. <p>What do you do now?</p>
#9	<p>Players consult IT to diagnose hardware issues.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 10: The slowness is not caused by a hardware issue. <input type="checkbox"/> <= 10: It is uncertain whether the slowness is caused by the hardware. <p>What do you do now?</p>
#10	<p>Players consult IT to diagnose network issues.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Before <i>Timed Inject #2</i>:</p> <p>There is a spike in network activity, but it does not appear to be anything out of the ordinary. What do you do now?</p> <p>After <i>Timed Inject #2</i>:</p> <p>There is a significant spike in network activity. Based on historical activity, the spike is abnormal. IT identifies an attack on the field device network and quarantines it. What do you do now? Play for 1-2 more turns before ending the scenario.</p> <p>After <i>Timed Inject #3</i>:</p> <p>IT identifies an attack on the field device network and quarantines it. What do you do now? Play for 1-2 more turns before ending the scenario.</p>
#11	Players escalate with suspicion of a cyberattack to the wrong party as indicated in the response plan.	<p>Add 10 game minutes to game clock.</p> <p>What do you do now?</p>

Table 15. Scenario 3 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#12	Players escalate with suspicion of a cyberattack to the correct party.	<p>Before <i>Timed Inject #3</i>: IT identifies an attack on the field device network and quarantines it. What do you do now? Play for 1-2 more turns before ending the scenario.</p> <p>After <i>Timed Inject #3</i>: IT identifies an attack on the field device network. Unfortunately, the attacker has already infiltrated the entire network. IT shuts down the network for several days while investigating before restoring operations. What do you do now? Play for 1-2 more turns before ending the scenario.</p>

Source: FHWA.

6.4.3.4 Narrative Ending

Once players have completed gameplay, allow one turn for any post-scenario player-actions. Then review the player actions during gameplay and select the appropriate ending based on the “Player Action Summarized” column. Read the end of the scenario in the corresponding “Scenario Ending” column.

Table 16. Scenario 3 narrative ending.

Ending No.	Player Action Summarized	Scenario Ending
Ending #1	Players ran out of time and did not follow their organizations cybersecurity incident plan.	The entire network has become encrypted and is inoperable. Later that day, management receives an email from the attacker. The attacker claims they will disable the network and delete all data unless payment is sent to them within 48 hours.
Ending #2	The device slowness was identified as a cyberattack BEFORE Inject 3.	Operations personnel successfully reported the incident before the attacker gained a solid foothold in the system. The cyberattack was successfully mitigated.
Ending #3	The device slowness was identified as a cyberattack AFTER Inject 3.	The attacker successfully installed software onto the network that encrypted all data. IT was forced to shut down all systems to prevent further access of the system by the attacker. It is uncertain how much data the attacker was able to retrieve before being discovered.

Source: FHWA.

6.4.3.5 Scenario-specific Objectives

Now that the scenario has concluded, review the following scenario objectives, and discuss how player actions met or failed to meet them:

1. Operations personnel should be familiar with the procedures for who to contact when there is a suspected incident. According to the incident response plan, did operators correct notify the correct parties?
2. While some of the early signs of a ransomware attack are not obvious, and network slowdowns are common problems in any connected system, participants should be able to differentiate between a normal network slowdown due to software or hardware problems and a potential cyberattack within the time constraints for the scenario.

6.4.3.6 Evaluation and Scoring

Select the appropriate checklist items and add the score modifiers to establish the ending score.

Table 17. Scenario 3 evaluation and scoring.

Checklist Item	Score Modifier
Ending 1	-30
Ending 2	+20
Ending 3	-10
Positive ending at least 30 game minutes before the scenario time limit.	+10
Players identify the nature of the cyber incident.	+5
Players refer to incident response plan for procedures in responding to the cyber incident.	+15
Players escalate the cyber incident to a relevant PoC.	+5
Players attempt to mitigate the damage of the cyber incident.	+5
Players follow scenario closeout procedures according to incident response plan.	+5
Players consult with IT to diagnose the network issue.	+15
Players attempt to investigate the field hardware.	+5
Players attempt to investigate the traffic management or vender software.	+10
Players attempt workarounds to communicate with devices.	+5

Source: FHWA.

Total Score:

6.4.4 Wargame Exercise—Scenario 4

Time to complete exercise successfully: 120 game minutes

Scenario Selection Questionnaire Modifier Value:

6.4.4.1 Variations

This scenario assumes the agency's TMC receives travel times from an external party (ex: Waze) and displays it on appropriate signage. If the TMC does not display travel times or only receives travel times from physical hardware on the roadway, consider one of the following alternatives.

Alternative 1

The TMC receives wrong way driver detections from a 3rd party.

1. Use the Alternative Timed Narrative instead of the Default Timed Narrative.
2. Replace “traffic conditions” with “wrong way driver” throughout the scenario.
3. Replace “travel time” with “wrong way driver detection” throughout the scenario.

Alternative 2

The TMC receives either pedestrian crossing (jaywalking) or near miss detections from a 3rd party.

1. Use the Alternative Timed Narrative instead of the Default Timed Narrative. Replace “wrong way driver” with either “pedestrian crossing” or “near miss.”
2. Replace “traffic conditions” with “pedestrian crossing” or “near miss” throughout the scenario.
3. Replace “travel time” with “pedestrian crossing detection” or “near miss detection” throughout the scenario.

6.4.4.2 Timed Narrative

Table 18. Scenario 4 timed narrative—default narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	The TMC receives an anonymous call. The caller is complaining about estimated travel times on a sign. The travel time indicates it should take 5 minutes to go 5 miles, but in actuality the roadway is severely congested, and traffic is moving very slowly.
Inject 2 [50 game minutes]	The TMC receives multiple complaints about inaccurate travel time estimates.
Inject 3 [90 game minutes]	The 3 rd party services provider that provides travel times to the TMC issues a public statement that their systems have been compromised by a ransomware attack. According to their statement, they are working to resolve the issue, but no timeframe has been identified and any data stored on their systems may have been altered or stolen.

Source: FHWA.

Table 19. Scenario 4 timed narrative—alternative narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	The TMC receives notifications about a wrong way driver detection.
Inject 2 [50 game minutes]	The TMC receives multiple false wrong way driver detections from different locations.
Inject 3 [90 game minutes]	The 3 rd party services provider that provides wrong way driver detections to the TMC issues a public statement that their systems have been compromised by a ransomware attack. According to their statement, they are working to resolve the issue, but no timeframe has been identified and any data stored on their systems may have been altered or stolen.

Source: FHWA.

6.4.4.3 Random Narrative Injections

Select a randomized inject after players have taken their turn based on the “Player Action” column. Then read the “Resulting Narrative.”

Table 20. Scenario 4 random narrative injections.

Random Inject No.	Player Action	Resulting Narrative
#1	<p>Players examine traffic conditions using existing cameras.</p> <p>Add 10 game minutes to game clock.</p>	<p>Camera images suggest that conditions are normal, and that the posted travel time is incorrect.</p> <p>What do you do now?</p>
#2	<p>Players attempt to determine whether the incorrect traffic times are due to a sensor failure using traffic software.</p> <p>Add 10 game minutes to game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 15: Sensors appear to be working properly and sending status updates. Eliminate sensors as a possible cause. <input type="checkbox"/> 5-15: Software suggests sensors are working properly but players cannot be sure. <input type="checkbox"/> < 5: No-one can determine whether the sensors are at fault. <p>What do you do now?</p>
#3	<p>Players send a field crew to investigate nearby devices.</p> <p>Add 20 game minutes to game clock.</p>	<p>Field crews determine that sensors are not at fault. Players recall that they also receive travel times from a 3rd party provider.</p> <p>What do you do now?</p>
#4	<p>Players determine that traffic times are not linked to sensors and consult relevant contact to find out how data gets to signage.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Roll a D20 and add the modifier to the result.</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 13: The team is familiar with the system structure and recalls that traffic times are provided through a 3rd party service. The team finds the appropriate contact information for the 3rd party. <input type="checkbox"/> 7-13: The team is vaguely familiar with the system structure and recalls that traffic times are provided through a 3rd party service, but they cannot recall who. The team spends some time searching before finding the appropriate contact information for the 3rd party. Add 10 game minutes to game clock. <input type="checkbox"/> < 7: The person who set up the system is unavailable, and nobody else knows how it works. Players may try again after one turn of play. <p>What do you do now?</p>

Table 20. Scenario 4 random narrative injections (continuation).

Random Inject No.	Player Action	Resulting Narrative
#5	<p>Players escalate to IT as a possible cyberattack.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> ≥ 10: IT conducts a security scan of the network and detects no malware. However, IT notices broken network connections to the 3rd party provider used by the TMC. <input type="checkbox"/> < 10: IT conducts a security scan of the network and detects no malware. <p>What do you do now?</p>
#6	<p>Players contact IT for troubleshooting network connections.</p> <p>Add 10 game minutes to game clock.</p>	<p>IT support test external connections and discovers that connections to its third-party 3rd party provider are not responding.</p> <p>What do you do now?</p>
#7	<p>Players contact 3rd party provider.</p> <p>Add 20 game minutes to game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <p>The 3rd party provider acknowledges that they have been impacted by a ransomware attack, but they are currently unable to restore service. The provider is unable to provide a timeframe for when service will be restored.</p>
#8	<p>Players attempt to identify alternative sources of travel time data.</p> <p>Add 10 game minutes to game clock.</p>	<p>Players work with IT support to disconnect from the 3rd party service provider and leverage alternative sources of travel time data. Travel times are not updated as frequently, but data is relatively accurate.</p> <p>What do you do now?</p>
#9	<p>Players blank out signs.</p>	<p>No travel times show on signage.</p> <p>What do you do now?</p>
#10	<p>Players ignore detections.</p>	<p>Players can no longer receive detections from third party.</p> <p>What do you do now?</p>

Source: FHWA.

6.4.4.4 Narrative Ending

Once players have completed gameplay, allow one turn for any post-scenario player-actions. Then review the player actions during gameplay and select the appropriate ending based on the “Player Action Summarized” column. Read the end of the scenario in the corresponding “Scenario Ending” column.

Table 21. Scenario 4 narrative ending.

Ending No.	Player Action Summarized	Scenario Ending
Ending #1	Players do not reach out to the 3 rd party provider, do not attempt workarounds to continue operations, and do not notify IT about the cyberattack of the external source.	Unless someone realizes that data is hosted on a third-party network, or detects that the connections are down, the issue cannot be resolved, and incorrect data will continue to be published. Since IT has not been notified of the potential cyberattack, the TMC is vulnerable via its connections to the 3 rd party.
Ending #2	Players do reach out to the 3 rd party provider, but do not notify IT about the cyberattack of the external source.	TMC personnel recognize the 3 rd party server as a possible source of faulty travel times and contact the service provider. The provider had not recognized the attack yet, and begins its mitigation, advancing the recovery time by several hours. The TMC cannot continue normal operations until the 3 rd party provider has recovered from the attack. Since IT has not been notified of the potential cyberattack, the TMC is vulnerable via its connections to the 3 rd party.
Ending #3	Players notify the 3 rd party provider of the problem. Players notify IT about the cyber attack	TMC personnel recognize the 3 rd party server as a possible source of faulty travel times and contact the service provider. The provider had not recognized the attack yet, and begins its mitigation, advancing the recovery time by several hours. The TMC operations are slowed until the 3 rd party provider has recovered from the attack.

Source: FHWA.

6.4.4.5 Scenario-specific Objectives

Now that the scenario has concluded, review the following scenario objectives, and discuss how player actions met or failed to meet them:

1. Players should be familiar with troubleshooting procedures regarding data provided by a 3rd party, such as verifying the 3rd party data and investigating the 3rd party network connection.
2. Players should be familiar with procedures for handling cyberattacks on a 3rd party or remote facilities as indicated in the incident response plan.
3. External dependencies should be known and documented. All systems impacting the TMC should be considered within the incident response plan. Operations staff should know which partners should be contacted to rectify this issue and be familiar with the correct point of contact in the external party.

6.4.4.6 Evaluation and Scoring

Select the appropriate checklist items and add the score modifiers to establish the ending score.

Table 22. Scenario 4 evaluation and scoring.

Checklist Item	Score Modifier
Ending 1	-30
Ending 2	+5
Ending 3	+20
Positive ending at least 30 game minutes before the scenario time limit.	+10
Players identify the nature of the cyber incident.	+5
Players refer to incident response plan for procedures in responding to the cyber incident.	+15
Players escalate the cyber incident to a relevant PoC.	+5
Players attempt to mitigate the damage of the cyber incident.	+5
Players follow scenario closeout procedures according to incident response plan.	+5
Players verify the issue using cameras or alternative data sources.	+10
Players contact IT to investigate.	+5
Players attempt workarounds to continue TMC operations.	+10
Players identify this as potentially an issue with a 3rd party provider and notify the provider.	+10

Source: FHWA.

Total Score:

6.4.5 Wargame Exercise—Scenario 5

Time to complete exercise successfully: 120 game minutes

Scenario Selection Questionnaire Modifier Value:

6.4.5.1 Variations

The following scenario assumes the agency’s traffic management center (TMC) manages Dynamic Message Signs (DMS). If the TMC does not operate DMS, consider the following alternatives.

Alternative 1

The TMC manages traffic signals.

1. Replace “DMS” with “Traffic Signals” throughout the scenario.
2. Replace “DMS message” with “Traffic Signal is flashing” throughout the scenario.
3. Replace Timed Inject #2 with the following:
 - The TMC receives a phone call about the traffic signal being in flash.

Alternative 2

The TMC manages Closed-Circuit Television (CCTV) cameras.

1. Replace “DMS” with “CCTV cameras” throughout the scenario.
2. Replace “DMS message” with “camera footage of Rick Astley’s hit song ‘Never Gonna Give You Up’” throughout the scenario.
3. Replace Timed Inject #2 with the following:
 - Local media regularly references camera footage when discussing weather or traffic conditions. Media notices that the camera is showing a video of Rick Astley’s hit song “Never Gonna Give You Up” on repeat.

6.4.5.2 Timed Narrative

Table 23. Scenario 5 timed narrative.

Scenario Inject No.	Timed Narrative
Inject 1 [Start Time 0]	A contractor calls into the TMC, stating that they are troubleshooting a DMS sign. The contractor cannot access the DMS sign to run diagnostics and states that their password is not working. The contractor requests the device password.
Inject 2 [50 game minutes]	The TMC receives a phone call about the DMS sign showing the fake message “Zombies ahead.”
Inject 3 [90 game minutes]	Local news is reporting the issue on livestream. Multiple signs are now showing the fake DMS message.

Source: FHWA.

6.4.5.3 Random Narrative Injections

Select a randomized inject after players have taken their turn based on the “Player Action” column. Then read the “Resulting Narrative.”

Table 24. Scenario 5 random narrative injections.

Random Inject No.	Player Action	Resulting Narrative
#1	Players immediately give the contractor the device password or configurations.	Add 50 game minutes to game clock and proceed to Timed Inject #2
#2	Player refuses to give up the password and hang up.	Add 10 game minutes to game clock and proceed to Timed Inject #2
#3	Players try to verify the contractor’s information and that the contractor’s agency is legitimate. Add 10 game minutes to game clock.	Roll a D20 and add the modifier to the result: <input type="checkbox"/> > 10: Players cannot find the contractor’s company, but it could be a new contractor working with the agency. <input type="checkbox"/> <= 10: The contractor provides a legitimate contracting company for the agency. What do you do now?
#4	Players ask the contractor which password they are using.	Roll a D20 and add the modifier to the result: <input type="checkbox"/> > 15: The contractor provides a known old password. <input type="checkbox"/> 5-15: The contractor provides the default password for the device. <input type="checkbox"/> < 5: The contractor provides a random password. What do you do now?

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Table 24. Scenario 5 random narrative injections (continuation)

Random Inject No.	Player Action	Resulting Narrative
#5	<p>Players escalate the call to the TMC operations manager.</p> <p>Add 10 game minutes to game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 15: The manager tells players not to give the password and the contractor’s supervisor must go through the appropriate channels for the password. The manager reports the contractor as suspicious. <input type="checkbox"/> 5-10: The manager tells players not to give the password and the contractor’s supervisor must go through the appropriate channels for the password. <input type="checkbox"/> < 5: The manager tells the player to give the contractor the password. <p>What do you do now?</p>
#6	<p>After refusing to give the password, players report the call to IT.</p>	<p>IT reports that the contractor is not known. Add 10 game minutes to game clock.</p>
#7	<p>Players attempt to fix the issues with the device remotely.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Roll a D20 and add the modifier to the result:</p> <ul style="list-style-type: none"> <input type="checkbox"/> > 10: The traffic software has an error whenever it tries to change the password. The software says, “unable to authenticate.” <input type="checkbox"/> <= 10: The traffic software claims to have successfully changed the message on the DMS. The TMC later receives another phone call about the sign. Add 20 game minutes to game clock. <p>What do you do now?</p>
#8	<p>Players send road crews to manually restore the DMS.</p> <p>If modifier is +2 or greater, add 10 game minutes to the game clock.</p> <p>Otherwise, add 20 game minutes to the game clock.</p>	<p>Road crews manually restore the sign.</p>
#9	<p>After restoring the DMS sign, players change the password.</p>	<p>The sign continues to function as normal.</p> <p>Play for 1-2 more turns before ending the scenario.</p>
#10	<p>Players escalate the password issue to IT with suspicion of a cyberattack.</p>	<p>IT examines all devices to ensure that no device has the same password.</p>

Source: FHWA.

6.4.5.4 Narrative Ending

Once players have completed gameplay, allow one turn for any post-scenario player-actions. Then review the player actions during gameplay and select the appropriate ending based on the “Player Action Summarized” column. Read the end of the scenario in the corresponding “Scenario Ending” column.

Table 25. Scenario 5 narrative ending.

Ending No.	Player Action Summarized	Scenario Ending
Ending #1	Players shared the password and did not do anything else before running out of time.	The attacker was able to change the administrative password on the sign. As a result, operators were locked out of the sign control. Eventually operators are locked out of multiple signs. IT support is unsure of what caused the issue.
Ending #2	Players shared the password and sent road crews to restore the device but did not change the password.	The attacker was able to change the administrative password on the sign. As a result, system operators were locked out of the sign control. Eventually operators are locked out of multiple signs. Restoring the device temporarily restored functionality, but soon the sign is showing the wrong message again.
Ending #3	Players shared the password, sent road crews to restore the device, and changed the password. Players do not escalate to IT.	The attacker was able to change the administrative password on the sign, but personnel were able to restore functionality to the device. Soon the TMC is receiving calls about a wrong message on a different sign.
Ending #4	Players shared the password, sent road crews to restore the device, changed the password, and escalate to IT.	The attacker was able to change the administrative password on the sign, but personnel were able to restore functionality to the device. Several DMS signs are showing the wrong message before IT changes their passwords.
Ending #5	Players refuse to provide the password but do not restore the device or change the password.	The attacker was able to change the administrative password on a single sign. As a result, operators were locked out of the sign control. IT support is unsure of what caused the issue.
Ending #6	Players do not share the password and sent road crews to restore the device but did not change the password.	The attacker was able to change the administrative password on the sign. As a result, system operators were locked out of the sign control. Restoring the device temporarily restored functionality, but soon the sign is showing the wrong message again.

Table 25. Scenario 5 narrative ending (continuation).

Ending No.	Player Action Summarized	Scenario Ending
Ending #7	Players do not share the password, sent road crews to restore the device, and changed the password. Players do not escalate to IT.	The attacker was able to change the administrative password on the sign, but personnel were able to restore functionality to the device.
Ending #8	Players do not share the password, sent road crews to restore the device, changed the password, and escalate to IT.	The attacker was able to change the administrative password on the sign, but personnel were able to restore functionality to the device. IT finds multiple devices using the same password and change those passwords to prevent similar attacks.

*Source: FHWA.***6.4.5.5 Scenario-Specific Objectives**

Now that the scenario has concluded, review the following scenario objectives, and discuss how player actions met or failed to meet them:

1. Operations personnel should be up to date on SLTT agency security policies, which cover email, phone conversations, and in-person interactions. Personnel should be able to recognize social engineering attempts and know not to give out password information over the phone or through email. Operations personnel should not share accounts and password complexity rules should be enforced. Personnel should also report suspicious calls to the appropriate party as indicated in the organization's incident response plan.
2. Players should be familiar with password management policies for devices.
3. Players should be familiar with procedures for restoring malfunctioning equipment.

6.4.5.6 Evaluation and Scoring

Select the appropriate checklist items and add the score modifiers to establish the ending score.

Table 26. Scenario 5 evaluation and scoring.

Checklist Item	Score Modifier
Ending 1	-30
Ending 2	-15
Ending 3	+5
Ending 4	+15
Ending 5	-20
Ending 6	-10
Ending 7	+10
Ending 8	+20
Positive ending at least 30 game minutes before the scenario time limit.	+10
Players identify the nature of the cyber incident.	+5
Players refer to incident response plan for procedures in responding to the cyber incident.	+15
Players escalate the cyber incident to a relevant PoC.	+5
Players attempt to mitigate the damage of the cyber incident.	+5
Players follow scenario closeout procedures according to incident response plan.	+5
Players are aware of password sharing policies within the organization.	+10
Players attempt to verify the contractor's company.	+5
Players should report the suspicious phone call.	+10
Players restore the device to a backup	+5
Players change the password on the device.	+5

Source: FHWA.

Total Score:

6.5 “After” Activities (Post-Exercise)

After the exercise, players should leverage exercise notes to review the exercise objectives and establish an evaluation score by completing the Exercise Evaluation Checklist. Based on these results, participants then develop an After-Action Report (AAR) with Improvement Plan (AAR/IP) to ensure any identified gaps or weaknesses are remediated.

6.5.1 Exercise Objectives

During the cybersecurity wargaming exercise itself, notetakers should observe all participants and take notes on relevant actions and discussions. Immediately after the wargame is complete, the participants should review and discuss the exercise. This includes reviewing exercise objectives and filling in the provided **Exercise Evaluation Guide Template** (section 9.5.1). Participants should evaluate their performance by discussing strengths and potential areas of improvement. This evaluation answers the following questions:

- Was the objective of the wargame exercise met?
- Based on current policies, how should participants have responded?
- What were some strengths and weaknesses identified by the wargame exercise?
 - If wargame exercise participants encountered specific challenges, what were they and why were they challenging?
 - How did the actions of participants compare with current policies and procedures?

6.5.2 Evaluation Metrics

Participants determine an evaluation score for the exercise by completing the Exercise Evaluation Checklist located after each exercise. Evaluation scores range from 100 to -30. An example evaluation can be found in **Example Evaluation** (section 9.4).



6.5.3 After-Action Report with Improvement Plan

Exercise leadership may begin drafting an After-Action Report after completing evaluation of the exercise. This report should include an exercise scenario overview, a description of the objectives tested, and a list of corrective actions. This report is used to communicate the results of the exercise to stakeholders.

The most important part of an AAR/IP is the list of corrective actions. These actions ensure that any weaknesses identified are remediated and can include changes to policy, organizational structure, and resources. These corrective actions should be based on the Exercise Evaluation Checklist and the EEG. If the agency will be publishing the AAR/IP, the evaluation team should be mindful to avoid disclosing weaknesses to the public. To ensure the corrective actions are addressed, each action should have an assigned responsible party and completion deadline for each corrective action.

Example Corrective Actions:

- Revise policies to ensure there is a designated point of contact that staff can report a suspected incident to. Familiarize personnel with the revised policies.
- Review incident response plan to familiarize personnel with appropriate procedures. Ensure response plan is easily accessible for all personnel.
- Develop password management policies for field devices. Default passwords should be changed, and each device should have a unique password.

After completing the AAR/IP, the participants should conduct an After-Action Meeting to review and distribute the AAR/IP. After this point the exercise leadership should regularly review the status of the corrective actions.

7. Conclusion

Everyone has different learning styles. This exercise offers something different from conventional classroom lectures by providing a game that teaches operations personnel in SLTT transportation agencies about the role of cybersecurity in their day-to-day work. This guide aims to help small, resource-constrained transportation agencies assess their current cybersecurity posture and identify potential changes to organizational policy. Larger organizations may use this guide to train small teams and new personnel.

Before planning a cybersecurity wargaming exercise, an SLTT agency should establish exercise objectives, stakeholders, and participants. The participants of the exercise should be operators and technicians involved in day-to-day operations of the agency representing their respective jobs.

To ensure this exercise can be run repeatedly by a single organization, this guide provides several different cybersecurity wargaming scenarios. These scenarios present different attack vectors that may be applicable to a SLTT agency and revolve around attacks on OT. This guide provides step-by-step instructions on selecting one of these scenarios, running a wargame with the selected scenario, and evaluating gameplay.

This guide also provides supplemental materials intended to aid gameplay and exercise evaluation, including cheat sheets, examples, and templates.

8. References

- Business Process Frameworks for Transportation Operations—FHWA Operations*. (n.d.). <https://ops.fhwa.dot.gov/tsmoframeworktool/>.
- Communications-Specific Tabletop Exercise Methodology | Office of Justice Programs*. (n.d.). <https://www.ojp.gov/ncjrs/virtual-library/abstracts/communications-specific-tabletop-exercise-methodology>.
- Costantini, L. P., & Raffety, A. (2021, October). *NARUC Cybersecurity Tabletop Exercise Guide*. pubs.naruc.org. Retrieved January 26, 2023, from <https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504>.
- Krause, C. (2019, September 17). *Cybersecurity and Intelligent Transportation Systems: Best Practice Guide*. <https://rosap.ntl.bts.gov/view/dot/42461>.
- USDOT ITS Research—About ITS Cybersecurity*. https://its.dot.gov/research_areas/cybersecurity/about.htm.
- Ramon, M. C. (2021, May 1). *Transportation Cybersecurity Incident Response and Management Framework: Cybersecurity Incident Exercise Summary Report*. <https://rosap.ntl.bts.gov/view/dot/57311>
- U.S. Department of Homeland Security. (2020, January). *Homeland Security Exercise and Evaluation Program HSEEP*. fema.gov. Retrieved January 26, 2023, from <https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf>.

9. Supporting Materials

The following section provides additional supporting examples, guides and tools to aid in players with this wargame exercise guide.

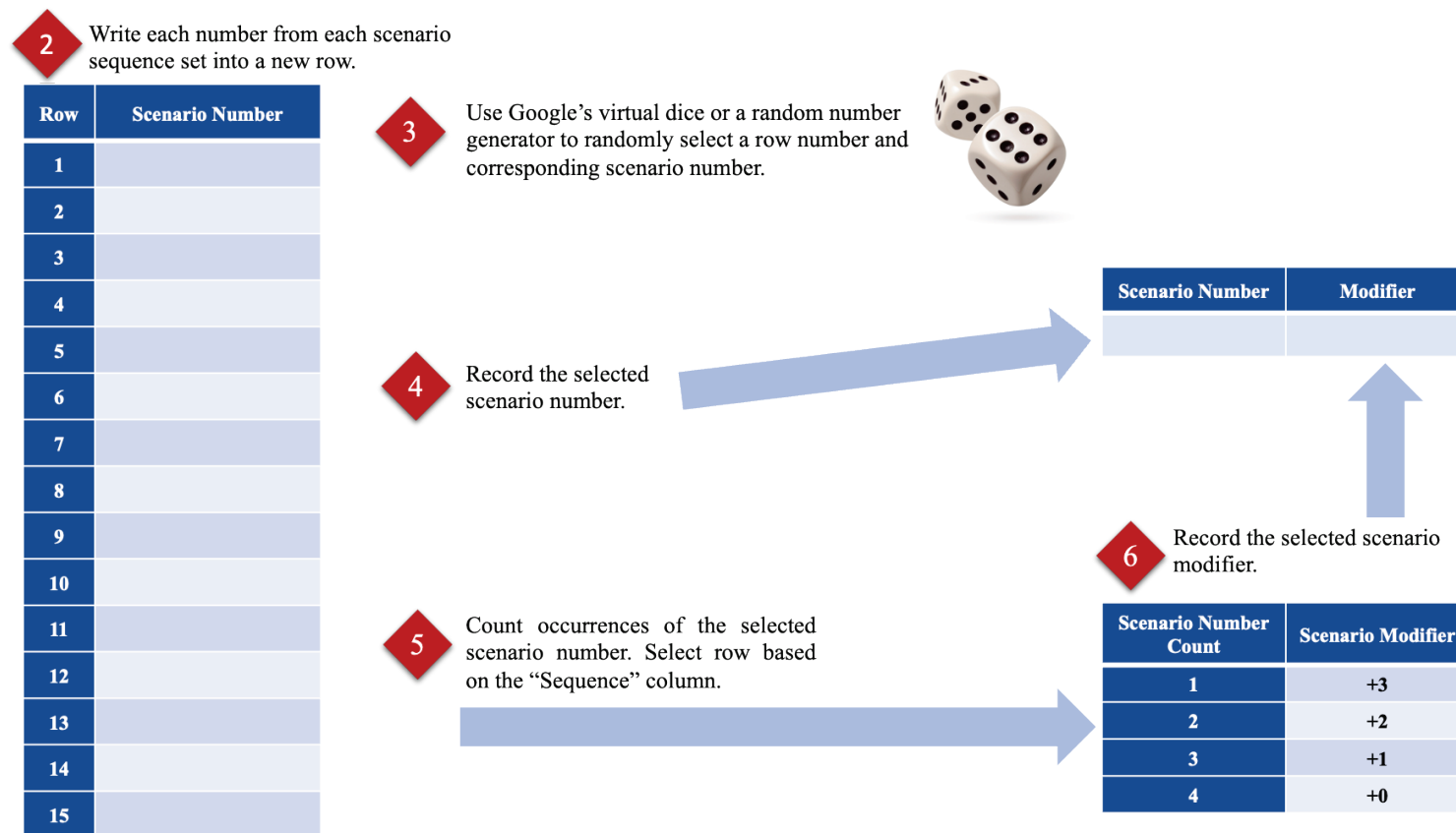
9.1 Visual Questionnaire Guide

#	Question	Scoring	Scenario Sequence Set
#1	Does your organization have a written policy on password management of field devices? What is the policy?	a. No policy on password management: Sequence Set = 5,5,1 b. Policy allows password reuse and/or sharing across devices, but does not allow default passwords: Sequence Set = 5,5 c. Policy does not allow password reuse and/or sharing across devices and does not allow default passwords: Sequence Set = 5	
#2	Does your organization manage Bluetooth devices (i.e., pedestrian crosswalks)? If so, are there any security policies for protecting these devices?	a. The organization manages Bluetooth devices, but there are no validation or encryption policies for communication with devices: Sequence Set = 2,2,2 b. The organization manages Bluetooth devices and does have validation and encryption policies for communication with such devices: Sequence Set = 2,2 c. The organization does not manage Bluetooth devices: Sequence Set = 1	
#3	Does your organization have policies for protecting against physical access of field devices? Does your organization perform regular backups of operations data?	a. If neither is done: Sequence Set = 3,1,1 b. If one is done: Sequence Set = 1,3 c. If both are done: Sequence Set = 1	
#4	Does your organization secure network communication with field devices?	a. There's no known network security policy: Sequence Set = 3,3,5 b. The field device network is segmented from the IT network: Sequence Set = 3,3 c. The field device network is segmented from the IT network, and network traffic is encrypted: Sequence Set = 3	
#5	Does your organization keep all its services on-site (i.e., no external or third-party service providers)? If not, what is the procedure if there are any issues with these external services?	a. A large portion of services are off-site, and there is no process for reporting issues: Sequence Set = 4,4,4 b. There are some off-site services, but there's a policy in place for reporting issues: Sequence Set = 4,4 c. There are no off-site services: Sequence Set = 5	



Source: FHWA.

Figure 5. Diagram. Example of questionnaire for scenario selection.



Source: FHWA.

Figure 6.Diagram. Example of scenario selection and scenario modifier.²

² Google’s virtual D20 <https://www.google.com/search?q=d20> or a random number generator <https://www.google.com/search?q=random+number+generator>.

9.2 Example Scenario Selection

As the first step in selecting an exercise scenario, the exercise leadership has organized all player(s) of the exercise into a meeting to complete the Scenario Selection Questionnaire. An example of this process showing the selected answer to each question is underlined in *figure 7*.

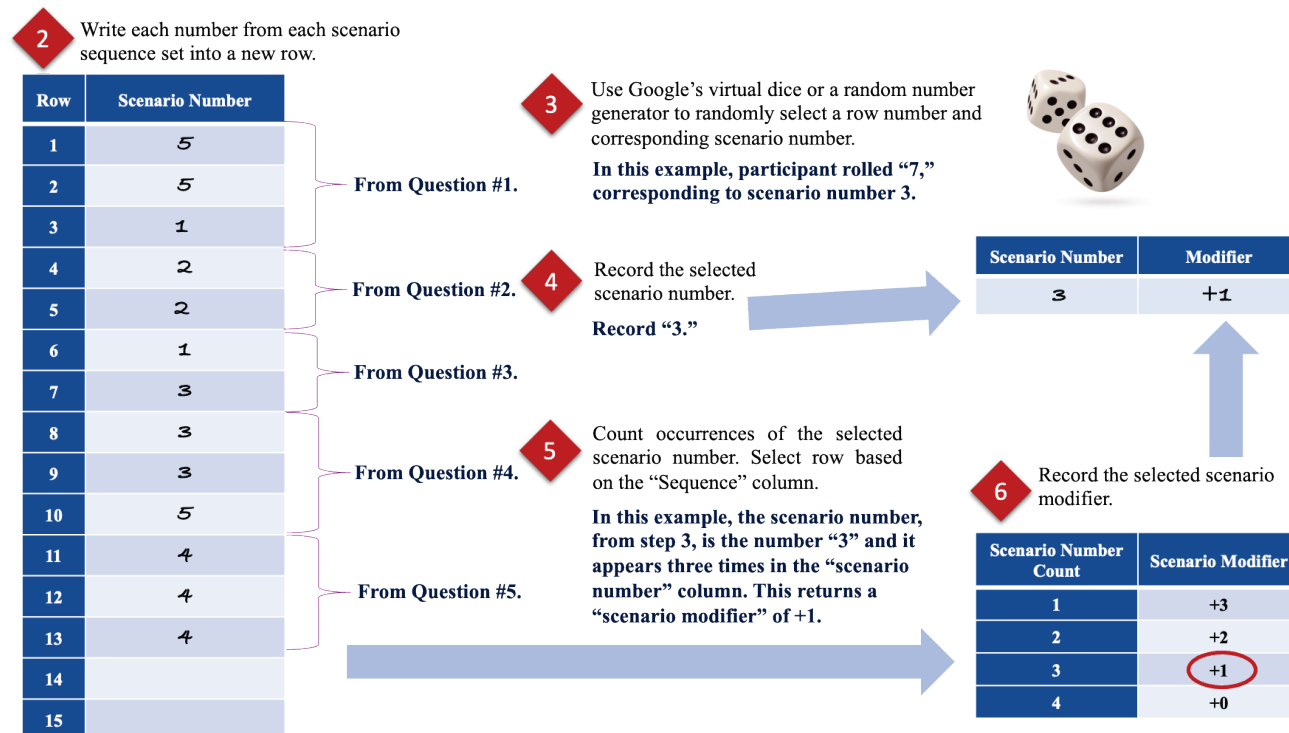


#	Question	Scoring	Scenario Sequence Set
#1	Does your organization have a written policy on password management of field devices? What is the policy?	<ul style="list-style-type: none"> a. No policy on password management: <u>Sequence Set = 5,5,1</u> b. Policy allows password reuse and/or sharing across devices, but does not allow default passwords: <u>Sequence Set = 5,5</u> c. Policy does not allow password reuse and/or sharing across devices and does not allow default passwords: <u>Sequence Set = 5</u> 	5, 5, 1
#2	Does your organization manage Bluetooth devices (i.e., pedestrian crosswalks)? If so, are there any security policies for protecting these devices?	<ul style="list-style-type: none"> a. The organization manages Bluetooth devices, but there are no validation or encryption policies for communication with devices: <u>Sequence Set = 2,2,2</u> b. The organization manages Bluetooth devices and does have validation and encryption policies for communication with such devices: <u>Sequence Set = 2,2</u> c. The organization does not manage Bluetooth devices: <u>Sequence Set = 1</u> 	2, 2
#3	Does your organization have policies for protecting against physical access of field devices? Does your organization perform regular backups of operations data?	<ul style="list-style-type: none"> a. If neither is done: <u>Sequence Set = 3,1,1</u> b. If one is done: <u>Sequence Set = 1,3</u> c. If both are done: <u>Sequence Set = 1</u> 	1, 3
#4	Does your organization secure network communication with field devices?	<ul style="list-style-type: none"> a. There's no known network security policy: <u>Sequence Set = 3,3,5</u> b. The field device network is segmented from the IT network: <u>Sequence Set = 3,3</u> c. The field device network is segmented from the IT network, and network traffic is encrypted: <u>Sequence Set = 3</u> 	3, 3, 5
#5	Does your organization keep all its services on-site (i.e., no external or third-party service providers)? If not, what is the procedure if there are any issues with these external services?	<ul style="list-style-type: none"> a. A large portion of services are off-site, and there is no process for reporting issues: <u>Sequence Set = 4,4,4</u> b. There are some off-site services, but there's a policy in place for reporting issues: <u>Sequence Set = 4,4</u> c. There are no off-site services: <u>Sequence Set = 5</u> 	4, 4, 4

Source: FHWA.

Figure 7. Example table. Completed questionnaire for scenario selection.

Together, the team continues to follow the scenario selection steps to determine scenario number and the modifier to use during gameplay. An example of this process is shown in *figure 8*.



Source: FHWA.

Figure 8. Diagram. Example of completed scenario selection and scenario Modifier.³

³ Google’s virtual D20 <https://www.google.com/search?q=d20> or a random number generator <https://www.google.com/search?q=random+number+generator>.

9.3 Example Scenario Gameplay

An example of scenario gameplay is provided. In the example, participants play through **Scenario 3** (*section 6.4.3*), starting at **Timed Inject 1** until **Timed Inject 2**. Instructions for scenario gameplay can be found in *section 6.3*. Text from the scenario is underlined.

9.3.1 Before Gameplay

After completing the *Scenario Selection Questionnaire* (*section 6.2*), players begin **Scenario 3** with a Modifier of **+1**.

Players start gameplay by reviewing the variations for Scenario 3. They decide to run the scenario using CCTV cameras.

9.3.2 Turn 1

The Game Clock is at 0 game minutes.

9.3.2.1 Inject Selection

Since the Game Clock is 0 game minutes, players select **Timed Inject 1**.



9.3.2.2 Inject

Players read **Timed Inject 1**:



While most devices seem to be operating normally, communication with several CTV Cameras of the same type seems to be slower than normal (i.e., timeouts, waiting for a response).

9.3.2.3 Player Action

1. Players typically use ATMS software to manage cameras on the roadway. They attempt to investigate the software to see if it could be the cause of the slowness.
2. In preparation for the next turn, the timekeeper adds 10 game minutes per the scenario instruction to the game clock (*section 6.3*).



Game Clock = 0 + 10 game minutes = 10 game minutes

3. Players begin the next turn.

9.3.3 Turn 2

The Game Clock is at 10 game minutes.

9.3.3.1 Inject Selection

1. Players select the random inject that most closely matches their action in Turn 1.
2. In this example, players select **Random Inject 2** after reading the corresponding Player Action:



Players attempt to determine if the slowness is caused by the software.

If modifier is +1 or less, add 10 game minutes to the game clock.

3. Since the gameplay modifier is +1, the timekeeper follows the instructions in the bolded text and adds 10 game minutes to the game clock.

Game Clock = 10 game minutes + 10 game minutes = 20 game minutes

9.3.3.2 *Inject*

1. Players begin reading the Resulting Narrative for **Random Inject 2** and read:

Roll a D20 and add the modifier to the result.

2. Using Google's virtual D20 (<https://www.google.com/search?q=d20>), players get a random number between 1 and 20. The virtual die rolls a 7. Adding the gameplay modifier of +1, their result is 8.
3. Players continue reading the Resulting Narrative based on the result from the previous step:

It is uncertain whether the slowness was caused by the software. What do you do now?

9.3.3.3 *Player Action*

1. Players are not sure what could be wrong and, after some discussion, decide to reach out to their ATMS provider.
2. In preparation for the next turn, the timekeeper adds 10 game minutes per the scenario instruction to the game clock.

Game Clock = 20 game minutes + 10 game minutes = 30 game minutes

3. Players begin the next turn.

9.3.4 Turn 3

The Game Clock is at 30 game minutes.

9.3.4.1 *Inject Selection*

1. Players select the random inject that most closely matches their action in Turn 2. They select **Random Inject 4** after reading the corresponding Player Action:

Players reach out to the ATMS provider to narrow down the source of the slowness. **Add 10 game minutes to game clock.**

2. The timekeeper follows the instructions in the bolded text and adds 10 game minutes per the scenario instruction to the game clock.

Game Clock = 30 game minutes + 10 game minutes = 40 game minutes



9.3.4.2 *Inject*

Players read the Resulting Narrative for **Random Inject 4**:

The ATMS provider indicates that the slowness is not caused by the ATMS software. What do you do now?

9.3.4.3 *Player Action*

1. Players decide to attempt other workarounds for communicating with devices.
2. In preparation for the next turn, the timekeeper adds 10 game minutes per the scenario instruction to the game clock.

Game Clock = 40 game minutes + 10 game minutes = 50 game minutes

3. Players begin the next turn.



9.3.5 **Turn 4**

The Game Clock is at 50 game minutes.

9.3.6 **Inject Selection**

Because the Game Clock is at 50 game minutes, players begin reading **Timed Inject 2**.



9.3.7 **Ending**

Players continue gameplay until they reach a scenario ending, the Game Clock is at 120 game minutes, or players decide they are done with the scenario.

They then proceed to the scenario ending and complete the scenario evaluation (See *section 9.4* for an example).



9.4 Example Evaluation

As an example, participants complete **Scenario 3** in 80 game minutes out of a possible 120 game minutes and achieve **Ending 2**. Based on these results and player actions, participants select the appropriate checklist items, which are highlighted in the table below, and total the results.

Table 27. Example of Scenario 3 evaluation and scoring.

Checklist Item	Score Modifier	Running Total
Ending 1	-30	
Ending 2	+20	+20
Ending 3	-20	
Positive ending at least 30 game minutes before the scenario time limit.	+10	+30
Players identify the nature of the cyber incident.	+5	
Participant(s) refer to incident response plan for procedures in responding to the cyber incident.	+15	
Players escalate the cyber incident to a relevant PoC.	+5	+35
Players attempt to mitigate the damage of the cyber incident.	+5	+40
Players follow scenario closeout procedures according to incident response plan.	+5	
Players consult with IT to diagnose the network issue.	+10	+50
Players attempt to investigate the hardware.	+5	
Players attempt to investigate the software.	+5	
Players attempt workarounds to communicate with devices.	+10	+60

Source: FHWA.

Evaluation scores range from 100 to -30, with 100 being the best possible score and -30 being the worst possible score. In this exercise, the participants got a total score of 60.

Total Score:

9.5 Report Templates

Below are report templates to support various stages of the exercise.

9.5.1 Exercise Evaluation Guide Template

During the exercise, evaluators should record player actions chronologically and record any notes and observations. In the case of a single-participant exercise, the participant will have to objectively record their own actions to identify strengths and weaknesses. This record will guide the exercise evaluation.

Evaluators should also store notes based on the discussion immediately after execution of the exercise. During this discussion, participants should give feedback on the exercise and discuss strengths and potential areas of improvement.

Top Strengths:

- 1.
- 2.
- 3.

Top Weaknesses:

- 1.
- 2.
- 3.

Source: FHWA.

Figure 9. Sample Layout. Template to capture top strengths and weaknesses.

The evaluation guide should consist of each objective in the exercise scenario and observations that address both positive and negative feedback. Evaluators may also wish to fill out an EEG before the exercise detailing the optimal approach to each objective.

Objective #[X]: [Objective Name]		
Objective: [Objective Description]		
Observations of Capabilities that Address the Objective	Notes for Improvement	Time of Observation

Source: FHWA.

Figure 10. Sample Layout. Template to capture observations and notes on objectives.

Evaluators should also record other observations and recommendation based on the notes taken during the exercise.

Observation	Notes or Recommendation

Source: FHWA.

Figure 11. Sample Layout. Template to record other observations, notes, and recommendations.

9.5.2 After-Action Report/Improvement Plan Template

[Exercise Name]

After Action Report/Improvement Plan

[Date of Report]

This After-Action Report/Improvement Plan (AAR/IP) is based on a Cybersecurity Wargaming Exercise conducted by [Agency Name] on [Date of Exercise] with [List of Participants]. This report provides an overview of the goals/objectives of the exercise, describes the scenario used to test capabilities, and suggests corrective actions to improve. Due to the sensitive nature of the topics being discussed, this report is designated as For Official Use Only and may not be distributed without written permission from [Name].

Objective: [Objective 1]

Strengths	[Strength 1] [Strength 2] [Strength 3]
Area(s) for Improvement	[Area for Improvement 1] [Area for Improvement 2]

Improvement Plan:

Issue(s)/Area(s) for Improvement	Corrective Action(s)	Due Date
[Area for Improvement 1]	[Corrective Action 1]	[Date to Complete]
	[Corrective Action 2]	[Date to Complete]
	[Corrective Action 3]	[Date to Complete]
[Area for Improvement 2]	[Corrective Action 1]	[Date to Complete]
	[Corrective Action 2]	[Date to Complete]

Source: FHWA.

Figure 12. Sample Layout. Template for after-action report/Improvement plan.

9.6 Exercise Game Mats

Below are exercise visual guides and game boards or mats to support participants as they go through scenario gameplay.

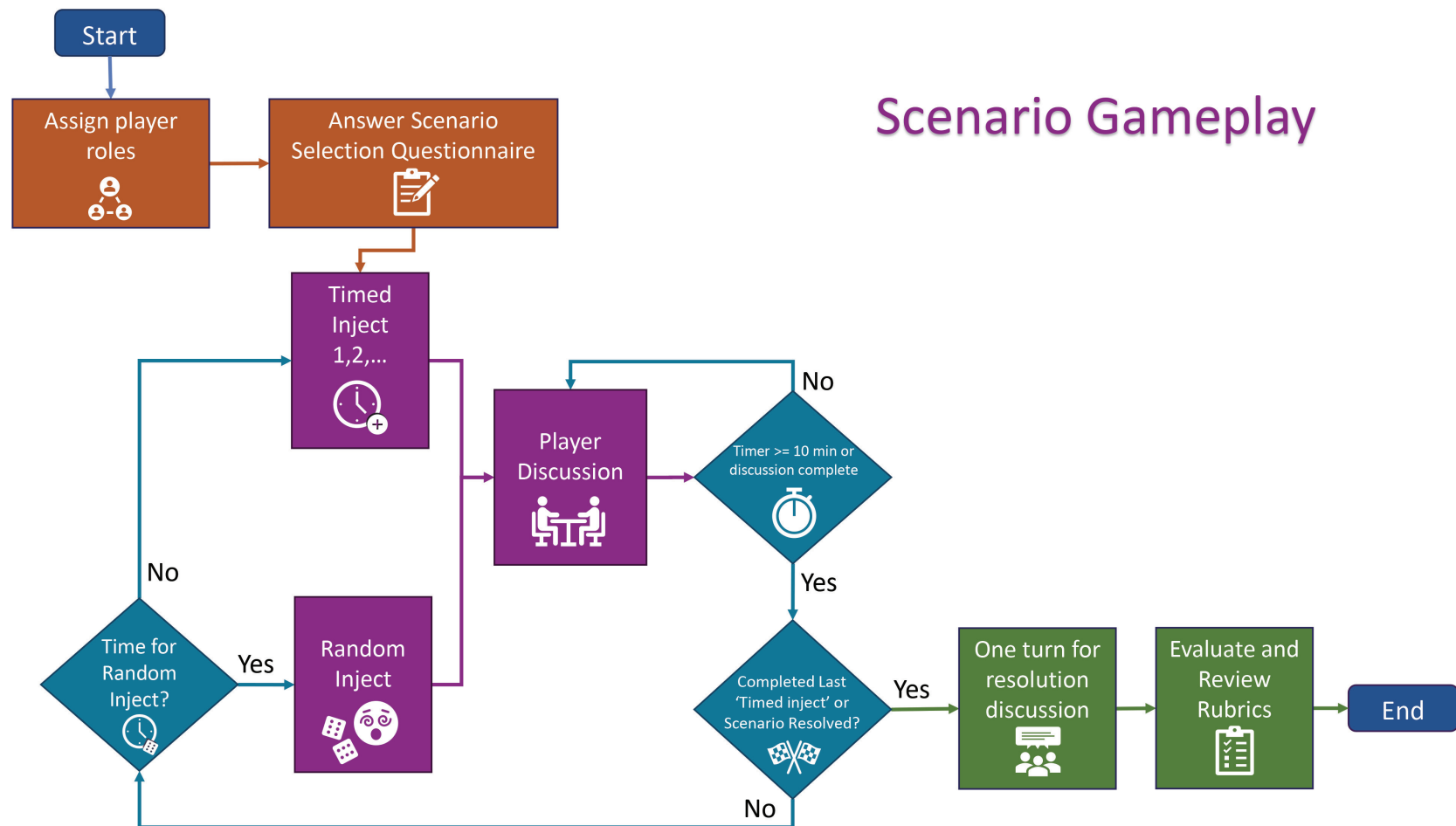
9.6.1 Cheat Sheets

Assign roles before gameplay (player, notetaker, timekeeper, and facilitator).

1. Run through the scenario selection questionnaire to determine two things:
 - Scenario #
 - Modifier
2. Play:
 - Start with timed inject 1 at Time=0
 - After any timed or random inject, run one round of discussion.
 - One round should take no longer than 10 minutes.
 - Add time of 10 minutes to game clock actions.
 - After a round of discussion
 - If game clock is not on a timed inject, run an applicable randomized inject.
 - If game clock is on a timed inject or there is not an applicable randomized inject, run next timed inject.
 - Once players have completed the last timed inject and feel they have finished the scenario, run one last round of discussion before moving on to Evaluation.
3. Evaluate (*section 6.5*)
 - Review the various endings and select the most applicable one.
 - Discuss how closely players met objectives.
 - Review evaluation rubric

Remember

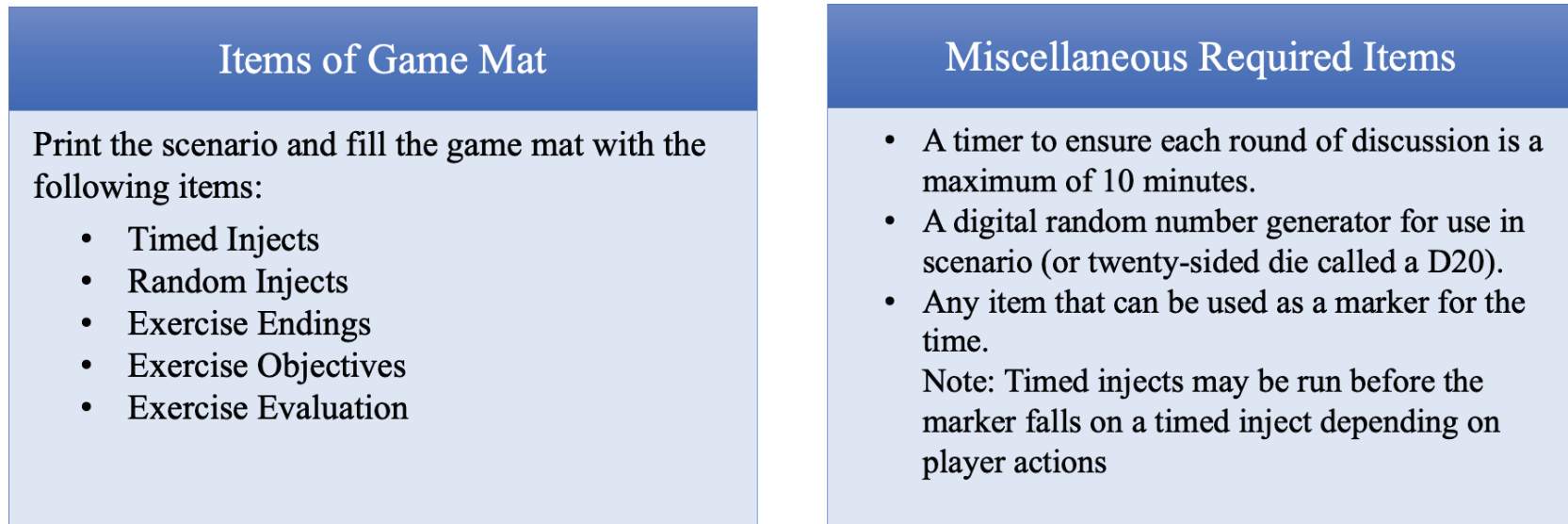
- DO NOT CHEAT (this is for you)
- No fault/no blame gameplay



Source: FHWA.

Figure 13. Flow chart. Scenario gameplay.

9.6.2 Gaming Mats for Facilitators



Source: FHWA.

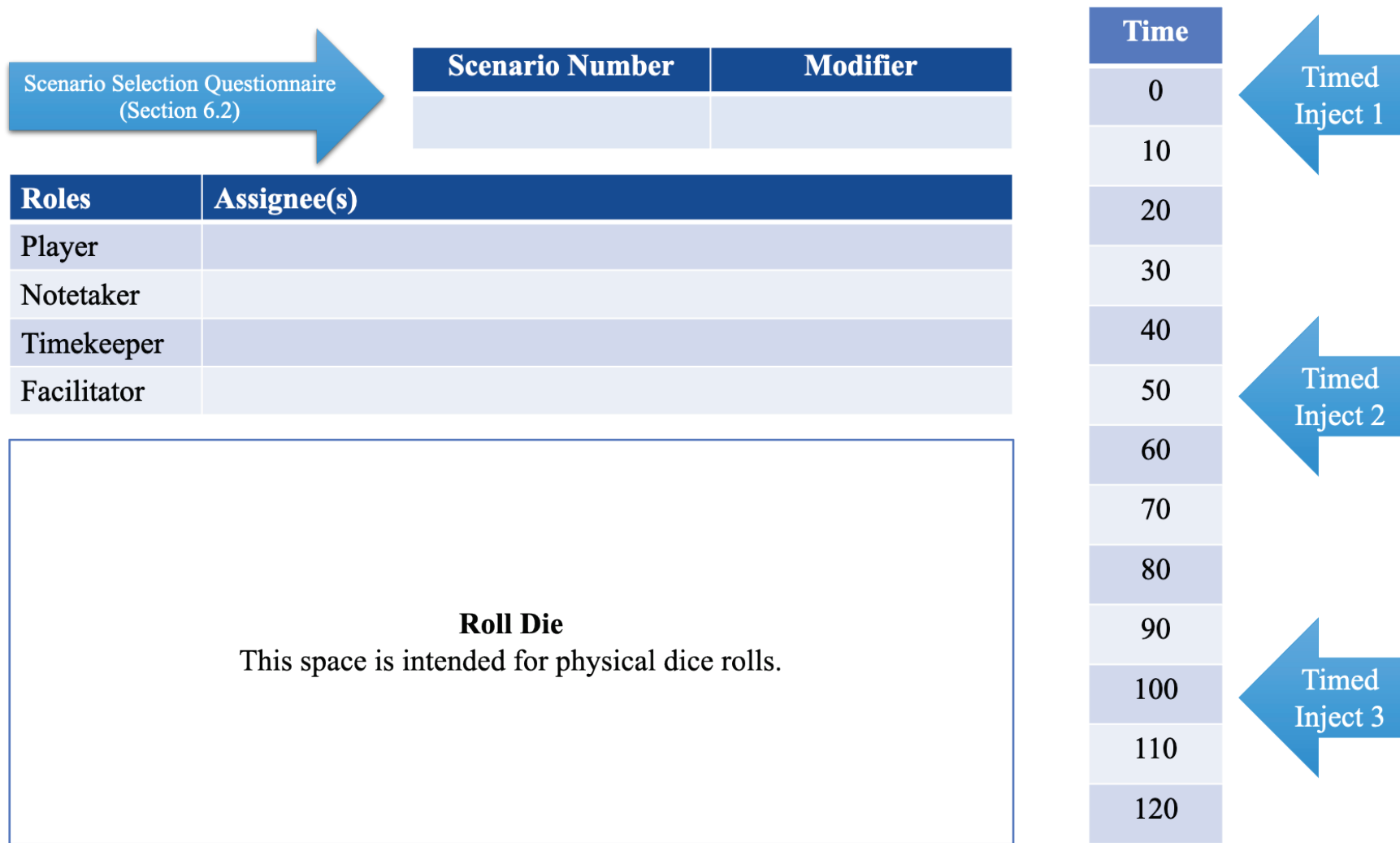
Figure 14. Diagram. Game facilitator reminders.⁴

Table 28. Quick reference of document section numbers for each scenario.

Section Numbers of Scenarios in Exercise Guide				
Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
6.4.1	6.4.2	6.4.3	6.4.4	6.4.5

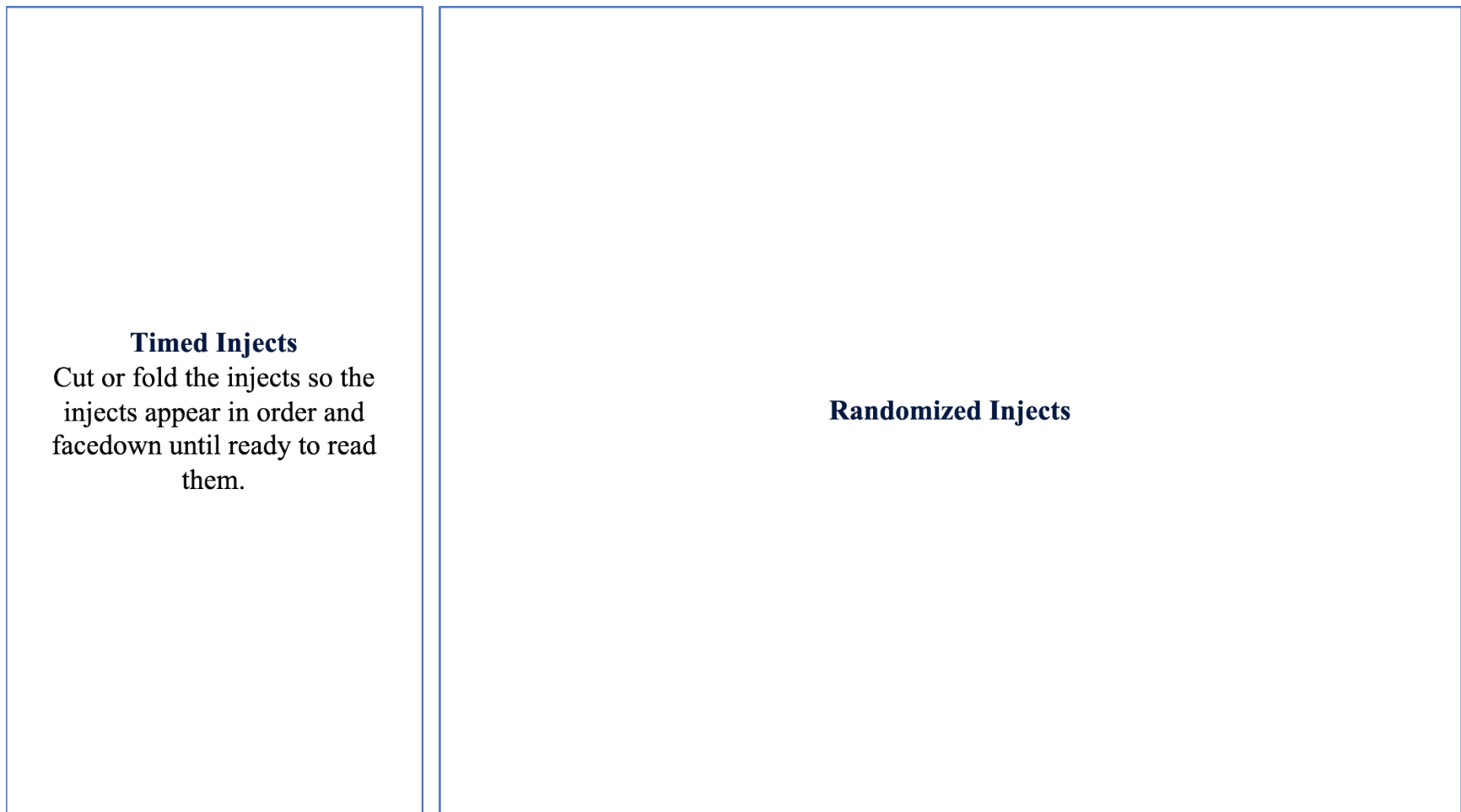
Source: FHWA.

⁴ Google’s virtual D20 <https://www.google.com/search?q=d20> or a random number generator <https://www.google.com/search?q=random+number+generator>



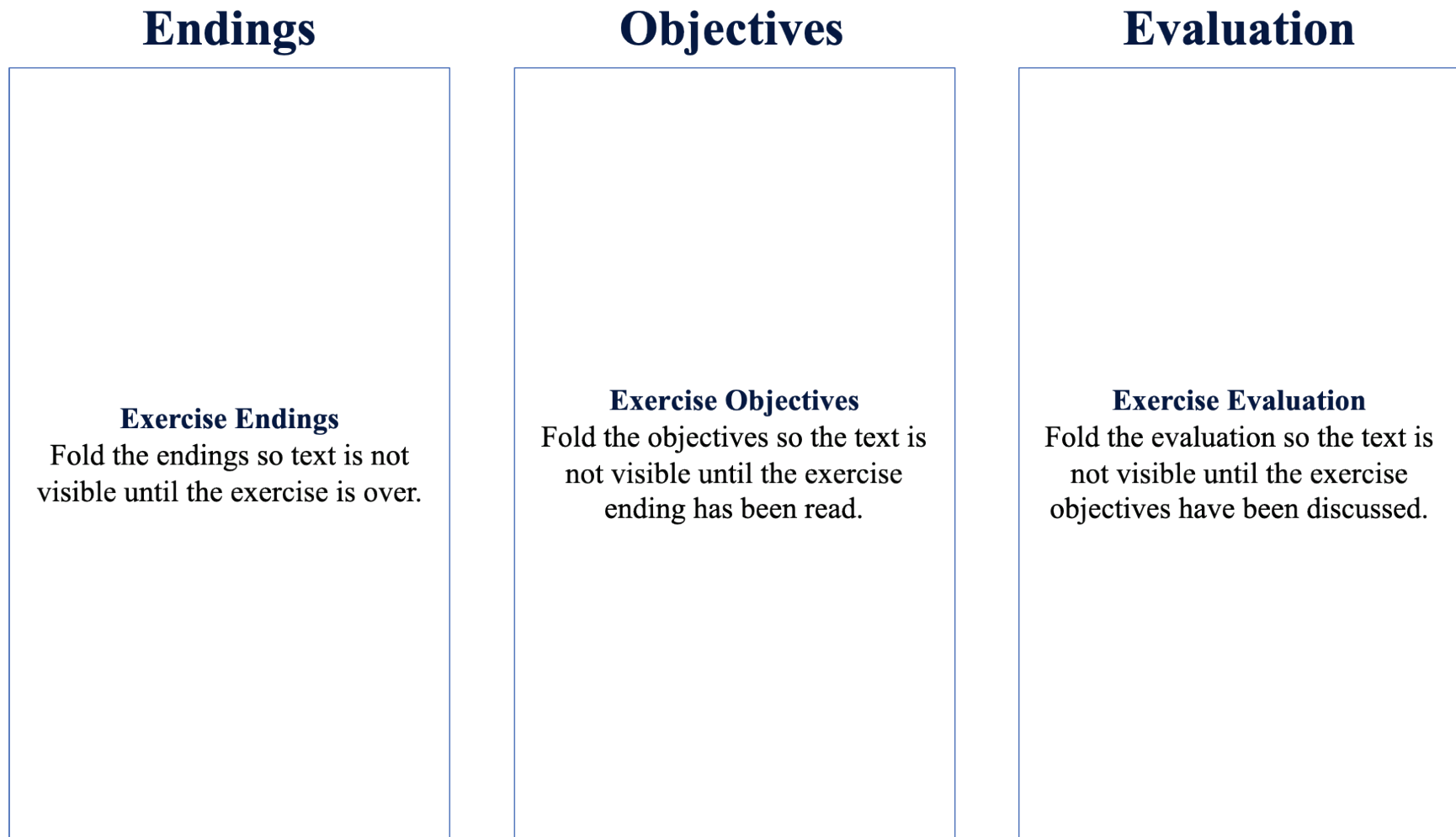
Source: FHWA.

Figure 15. Representation. Wargame exercise—gameplay mat.



Source: FHWA.

Figure 16. Representation. Wargame exercise—timed injects mat.



Source: FHWA.

Figure 17. Representation. Wargame exercise—endings, objectives, and evaluation mat.

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-24-137



U.S. Department of Transportation