Emergency Services Sector Tabletop Exercise

Situation Manual

[Insert Date]

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Photo Courtesy of DHS

This page is intentionally left blank.

EXERCISE AGENDA

Time	Activity
0800 – 0830	Registration
0830 – 0900	Welcome and Introductions
0900 – 0950	Module One – Threat Buildup
0950 – 1000	Break
1000 – 1055	Module Two – Response
1055 – 1105	Break
1105 – 1200	Module Three – Continuity of Operations
1200 – 1230	Hot Wash

*All times are approximate

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Emergency Services Sector Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters]. This exercise was developed using materials created by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select applicable Mission Areas]
Core Capabilities	Planning; Intelligence and Information Sharing; Risk Management for Protection Programs and Activities; and, Public Information and Warning [insert other core capabilities]
Objectives	1. Assess information sharing capabilities with the public, sector partners, and Federal, State, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 2. Review intelligence and information sharing and dissemination processes in relation to a credible threat to critical infrastructure owners / operators. 3. Discuss private sector stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under National Incident Management System (NIMS) with local, State, and Federal agencies. 4. [Insert additional exercise objectives as necessary]
Threat or Hazard	Cyber and Vehicle-Borne Improvised Explosive Device (VBIED)
Scenario	This scenario is an interactive, discussion-based activity focused on a cyber security incident and VBIED attack. The scenario consists of three modules: Threat Buildup, Response, and Continuity of Operations.

Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	[Insert a brief summary of the total number of participants and participation level (i.e., Federal, State, local, tribal, non-governmental organizations [NGOs], private sector, and/or international agencies). Consider including the full list of participating agencies in Appendix A. Delete Appendix A if not required.]
Points of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (e.g., exercise director or exercise sponsor)]

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The exercise objectives listed in Table 1 describe the expected outcomes from the TTX. These objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific prevention, protection, and response mission areas. The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
Assess information sharing capabilities with the public, sector partners, and Federal, State, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures.	✓ Planning ✓ Intelligence and Information Sharing ✓ Public Information and Warning
Review intelligence and information sharing and dissemination processes in relation to a credible threat to critical infrastructure owners / operators.	✓ Public Information and Warning ✓ Intelligence and Information Sharing
Discuss private sector stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under NIMS with local, State, and Federal agencies.	✓ Planning ✓ Risk Management for Protection Programs and Activities
[Insert additional objectives as necessary]	✓ [Insert additional core capabilities as necessary]

Table 1.—Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Types of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers.** Observers do not directly participate in the exercise; however, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts (SMEs) during the exercise.

- **Evaluators.** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

Exercise Structure

This TTX is comprised of three modules consisting of a cyber attack and VBIED and their aftermath. Players will participate in the following module elements:

- Module One: Threat Buildup
- Module Two: Response
- Module Three: Continuity of Operations

Each module begins with a scenario update that summarizes the key events occurring within that time period. A series of questions following the scenario summary will guide the facilitated discussion of critical issues in each of the modules. Based on exercise priorities, time dedicated to each module will be managed by the facilitator.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- The situation updates, written material, and resources provided are the basis for discussion. There are no hidden materials or scenarios.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, and response efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively affect their participation. During this exercise, the following apply:

- The scenario for this exercise is fictitious and does not represent any actual intelligence.
- The scenario is plausible, and events occur as they are presented.
- There are neither "hidden agendas" nor any "trick questions."
- All players receive information at the same time.

- Assume cooperation and support from other responders, agencies, and organizational entities.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities, capability targets, and critical tasks. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the After-Action Report (AAR).

This page is intentionally left blank.

MODULE ONE: THREAT BUILDUP

Date: [Insert Event Date -2 months]
Location: [Insert Facility Name and Location]

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) alert issued on threat similar to Stuxnet

A research lab with strong international connections alerts the cyber community to a malware sample that appeared to be very similar to Stuxnet and creates files with the file name prefix "~DQ". The research lab provided samples recovered from computer systems in Europe, as well as a detailed report with their initial findings, including analysis comparing the threat to Stuxnet, which have been confirmed.

Parts of the malware are nearly identical to Stuxnet, but with a completely different purpose. The new malware is essentially the precursor to a future Stuxnet-like attack. The threat was written by the same authors (or those that have access to the Stuxnet source code) and appears to have been created since the last Stuxnet file was recovered. The new malware's purpose is to gather intelligence data and assets from entities, such as communication infrastructures, utility control facilities, and other infrastructure control mechanisms, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on this type of infrastructure.

The malware does not contain any code related to industrial control systems and is primarily a Remote Access Trojan (RAT). The threat does not self-replicate. Telemetry shows the threat was highly targeted toward a limited number of organizations for their specific assets. However, it is possible that other attacks are being conducted against other organizations in a similar manner with currently undetected variants.

Technical Community is Aware of Vulnerability in Industrial Control Systems [1]

A few months ago, a rather apocalyptic blog was published on the *XyozaNet* portal. The blogger stated, "*cybersecurity experts have discovered that many of the systems that control infrastructure in the U.S. have vulnerabilities that, if exploited, could dramatically alter our way of life*."

The blog generated heavy internet traffic. Many of the responses were even more cryptic than the original blog. Others expressed doubt about the doomsday scenario – "W*hat do those systems have to do with me? I don't work in anything involving infrastructure. I'm not losing any sleep over this one!*" In contrast, one short response made a simple point: "*Not news. Not a secret. Issue has been worked on for years. Check out NSTB at INL.*" In fact, the original blog was spinning publicly available reports from Idaho National Laboratory (INL) and other sources.

[1] Energy control systems are the mechanisms that operate and monitor energy infrastructure. Two examples of such systems are the supervisory control and data acquisition (SCADA) and the distributed control systems (DCSs)

Increased Threat of Domestic Terrorism and Other Law Enforcement Concerns

The [State or Regional] Fusion Center has received updated intelligence analysis bulletins from its Federal partners that reflect concern about the growing sophistication of, and cooperation among, domestic groups involved in environmental, cyber, and economic terrorism.

Over the last few months, the Fusion Center and local law enforcement agencies have been exchanging notes about their shared concerns resulting from the inflammatory rhetoric of a loose network of independent information technology (IT) professionals who became actively involved in the blogosphere discussions surrounding the [Insert local Public Service Companies'] labor contract negotiations. Local law enforcement receives a tip suggesting that some of these individuals are utility contractors.

National Lab Discovers Vulnerabilities in supervisory control and data acquisition Systems Used by Natural Gas Industry

- Over the last decade, as part of INL's National Supervisory Control and Data Acquisition Test Bed (NSTB) program, government experts, utility companies, and other private sector partners have conducted rigorous security assessments of digital control systems that could put such systems at risk for a cyber attack.
- The types of vulnerabilities discovered ranged from conventional IT security issues to specific weaknesses in control system protocols.
- These systems in question ranged in complexity from a perimeter protection device, to small digital control systems, to large supervisory control and data acquisition / energy management systems with complex networks, multiple servers, and millions of lines of code.

Newly Identified SCADA Vulnerability Triggers ICS-CERT Alert

A vulnerability in a SCADA protocol was identified and publicized by *QyteBlox*, a small IT security firm in Alberta, Canada. The protocol in question is used in control systems for monitoring power output and efficiency throughout all portions of the electricity generation and distribution systems.

The security manager from a Canadian electricity distribution company shared the information from the *QyteBlox* blog posting with the Federal Energy Regulatory Commission. ICS-CERT issued an Alert on [insert Date - 6 weeks] regarding the SCADA vulnerability identified by *QyteBlox*. ICS-CERT noted that numerous electric utility organizations rely upon automatic

generation control systems to share generation supply and demand data between utilities and their respective Transmission System Operator (TSO).

The ICS-CERT alert was shared with and distributed by the Emergency Services Sector Information Sharing and Analysis Center (EMR-ISAC). SCADA systems vendors promptly initiated work to develop patches for the vulnerability.

The Federal Bureau of Investigation's (FBI) InfraGard picked up internet chatter regarding the SCADA vulnerability. Notably, there was intelligence suggesting that domestic groups have plans to target the patches being developed to address the vulnerability.

Discussion Questions

General Discussion Questions

1. What is the process by which your organization would receive intelligence and protective measure information given the threat described?
    a. What government organizations would you communicate with?
    b. Does your organization maintain a relationship with your Department of Homeland Security (DHS) Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
    c. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) website?
2. What internal information sharing and dissemination processes does your organization currently have in place?
3. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your personnel?
4. What resources are used to disseminate information?
    a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you use to share information and communicate protective measures implementation?
    b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing?
        i. If so, how will you distribute the threat information?
5. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
    a. Does your organization perform independent analysis on information provided? If so, describe the process.
6. In the event that your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to appropriate law enforcement entities?
    a. Would you also report this to any Federal partners?
7. If there is identified "suspicious activity" observed, how is this reported locally and within the Emergency Services Sector?
    a. Are trends of suspicious behaviors tracked across the Emergency Services Sector nationwide?
    b. Is your organization aware of the "If You See Something, Say Something™" campaign or the National Suspicious Activity Reporting (SAR) Initiative (NSI)?

8. Given evidence of a credible threat to the energy sector, and that any attack on that sector would directly affect the Emergency Services Sector, what elements in a robust emergency response plan are important to have in place?
9. What protective security measures or recommendations, if any, will be employed at your organization following this threat?
    a. Do you coordinate protective measure implementation with any other organization within the Emergency Services Sector, or with government entities?
    b. How are the protective measures the Emergency Services Sector have put in place communicated back to the government?
    c. How useful are the information bulletins and advisories DHS provides (e.g., a Joint Intelligence Bulletin [JIB]) that recommend protective measures?

Cyber Specific Activities

1. Does your company have a formal / informal policy or procedures pertaining to IT account management?
    a. Do these policies or procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?
    b. Do these policies or procedures include protocols / steps for notifying IT account managers / administrators when users are terminated?
2. What policies or procedures does your company have in place to address cyber vulnerabilities or cyber threats?
3. What is your company's policy regarding information system access and terminated employees?
4. What information system-related property (e.g., authentication key, system administration's handbook / manual, keys, identification cards) does your company retrieve during the employment termination process?
5. How are information system violations addressed?
    a. Does your company employ a formal sanctions process for personnel failing to comply with established information security policies and procedures? If so, has this been communicated to the employees and how often?
6. What is your company's policy regarding information security training?
    a. How often is training provided?
    b. What is the training program for new employees?
    c. How often are IT managers, system and network administrators, and other IT personnel having access to system-level software required to receive training?
    d. How does your company track security training compliance?
    e. How can these policies be improved?

MODULE TWO: RESPONSE

Date: [Insert Date -1 Month]
Location: [Insert Facility Name and Location]

Cyber Attack Develops

An underground computer programmer with links to terrorist organizations has been able to secure the source code for the malware and craft a new variant. The programmer, named Randall Smith, has been involved in multiple hacking activities, although mostly on a smaller low impact scale. His greatest self-proclaimed accomplishment to date was his ability to reword, reroute, and/or cancel communications transmissions in a local security company, interfering with responses and sending security guards on searches for non-existent threats. Smith has expressed a deep-seated hatred for the United States. He has written that the United States should "mind its own business and keep its capitalist hands out of others' affairs." For some time he has been looking for a way to target the American infrastructure, which he feels, had grown too large and intrusive.

Smith has been an active blogger since 2010. He applauded the Stuxnet worm and vowed to help support additional efforts against infrastructure in the United States. He has been approached by terrorist organizations who desire his services, but no confirmation of him working for any terrorist group has yet to be discovered.

Smith utilized connections he made several years ago at DEFCON Hacking Challenge to help him plant the worm into the SCADA systems at [Insert Electric utility company] around early [Insert previous month]. As the worm went to work, he began collecting vital information on the SCADA systems that would allow him to wreak havoc on the wider electricity distribution systems.

Date: [Insert Date -1 day]
Location: [Insert location]

Service Disruption

8:05 p.m. [Insert Electric utility company] reported that six of its seven regional electrical distribution substations were experiencing severe overheating and electrical overload problems, as reported by the electrical utility company's control room. In response to this, these substations were taken offline, resulting in an electrical blackout for most of [Insert jurisdiction].

8:09 p.m. [Insert Electric utility company] received calls from their power generating stations stating that, due to a severe increase in steam pressure within the primary turbines, they were required to take the stations offline. This increase in pressure was detected by instruments in the power generating stations' control rooms. It is not known when the power generating stations will restart.

Date: [Insert Date – 1 day]
Location: [Insert location]

VBIED in the Business District

4:17 p.m. 911 started fielding calls with reports of an explosion that appeared to originate in a vehicle that was parked near [Insert restaurant area in business district]. This restaurant was unusually busy, with many people sitting in the outdoor dining section, due to the ongoing power outage. The reports also indicated many casualties, the extent and severity of which are still being assessed. Security cameras, which would normally enable a direct visual feed of the incident scene, did not function properly, perhaps due to the ongoing power outage.

4:24 p.m. A local police department patrol officer arrived on-scene. He reported that many of the apparently physically uninjured people at the scene reported trouble breathing, with most describing itchy throats, watering eyes, and constricted airways. Much of the area around the apparent blast site was burning steadily, without evidence of the flames rapidly spreading. The officer noted that his radio worked, but the computer uplink in his vehicle did not.

4:46 p.m. Fire department responders arrived on-scene. This unit was delayed due to the normal computer-based dispatching system being sluggish and nonresponsive.

4:48 p.m. Multiple ambulances, from all local ambulance companies, arrived at the scene. Almost every ambulance in the district was present; leaving some paramedics questioning the size of the response.

4:58 p.m. Hazardous Materials (HAZMAT) teams arrived in response to the odd symptoms reported by the first responding police officer and began sampling procedures to determine if any unusual hazardous materials are present.

Throughout the entire response, communications from the first responders to their headquarters elements were difficult at best, with many messages not being transmitted or arriving garbled. Additionally, developing a common operating picture at each agency, as well as at the emergency operation centers, was much more time consuming and less accurate than normal, due to the increased difficulty in obtaining real-time situation reports from responders.

Cybersecurity Breach Identified

IT personnel working alongside system controllers identified that the system operating the control systems at both the power-generating stations and the electrical distribution substation control centers were remotely compromised. Upon this assessment, the utility began switching to manual operations.

Operations are underway to isolate the causes of the power outage, and to balance the electrical grid through the distribution system to restore service to end users.

Additionally, although this has not yet been confirmed, evidence supports the hypothesis that the communications systems that support first responders and emergency operations centers may have been compromised as well.

Discussion Questions

General Discussion Questions

1. What are your organization's information sharing responsibilities during the response to the incident?

2. What formal information sharing processes would your organization use at this point?
3. Does your organization's emergency response plan contain protocol for responding to the incidents described in this module?
4. What resources are used to disseminate information?
    a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you use to share information and communicate the implementation of protective measure?
        i. Do these systems work when there is a widespread disruption of power? If not, are other systems available?
5. What protective security measures will be employed at your organization following these domestic attacks?
    a. Do you coordinate protective measure implementation with any other organization within the Emergency Services Sector or with government entities?
    b. How are the protective measures the Emergency Services Sector have put in place communicated back to the government?
    c. How useful are the information bulletins and advisories that DHS provides that recommend protective measures?
6. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance)?
7. Do your existing plans, policies, and procedures address counter-IED (C-IED) considerations?
    a. If not, are you familiar with the resources available through the DHS Office of Bombing Prevention to assist in incorporating C-IED measures into planning efforts?
8. Who is responsible for coordinating the risk communications message for your organization?
9. What are the key messages that should be distributed concerning the continuing credible threat to your organization and stakeholders?
    a. Is the message coordinated within the Emergency Services Sector?
    b. If so, what is the process for coordinating this message?
10. Would your organization review and update your emergency response plan after the response to these incidents was completed?

Cyber Specific Actions

1. What types of cybersecurity policies, plans, and/or protocols does your company have in place to detect, respond to, and/or recover from a cyber attack?
2. Whom would you contact about the cyber incident?
    a. Internally?
    b. Externally?

3. What internal and external messages should be developed? How are they being distributed?
4. What are the business implications of the scenario? How would you determine them?
5. Would you contact customers? If so, how is your firm's public relations department involved? What role would you have in shaping the messages for customers and media inquiries?
6. At what point would you contact law enforcement when dealing with a cyber attack?
7. What protocols exist in your firm to address such an event?
8. Do you have detection, triage, and response capabilities?
9. Do employees know what constitutes suspicious cybersecurity activities or incidents? Do they know what actions to take when one arises?
10. Would this incident trigger contact with regulators, or other government oversight organizations? Why or why not?
    a. When would such contact occur?

MODULE THREE: CONTINUITY OF OPERATIONS

Date: [Insert Incident + 10 days]
Location: [Insert Facility Name and Location]

The power outage that began on [Insert Incident – 1 day, from Module 2] took over three days to partially resolve, which resulted in rolling blackouts throughout much of the city, and another five days for the city to return to normal operations. Of the six regional electrical distribution substations that were initially taken offline, four have been returned to full operation; the other two were discovered to have been physically damaged by gunshots to their radiators, allowing the oil to leak out and cause actual overheating of the systems. These transformers will take many weeks to replace and will cost the utility company in excess of $16 million dollars.

The communications systems used by first responders were definitely compromised by a Trojan-type virus similar to the one created by Randall Smith, whose whereabouts are still unknown. In order to fix the systems, it is necessary to take all potentially effected communications systems offline. The lack of power and communications are hampering the ability for local government to be "at the ready."

Because of severe traffic congestion due to inoperable traffic control devices and limited communications, emergency responders are having problems traveling to accident and incident sites.

In response to and fear of the bombing, 911-type call volume in the area has greatly increased causing the phone companies to "block" lines where phone lines are still operational. The "blocking" of lines is necessary to allow first responders primary access. Some first responders are trying to use their satellite phones but not all are working properly, while others are not familiar with how to use them. The 'walkie-talkie" or push-to-talk systems are generally the most consistent form of communication. This could be a problem later when batteries run low and there is no power to recharge them.

The media is on-scene reporting on damage and inquiring about the validity of actions, both in response to the cyber attack and bombing, and in relation to the ability of emergency responders to quickly and efficiently handle emergencies in the near future.

Discussion Questions

General Discussion Questions

1. At this point in the scenario, what does the emergency response structure look like?
    a. Does it provide avenues for public-private coordination?
2. What information would be exchanged between government and critical private sector partners?
    a. What information is required at this point?
    b. What method(s) of communication would your organization use to communicate?

   c. Does your organization have access to emergency response and continuity plans for the organizations you depend on? How familiar are you with their plans and their effect on your organization?

   d. Would the method of communication change as the event evolved?

3. Do you have a formalized process for managing data?

   a. What information platforms are still used? Are they still viable when normal communications methods are unavailable?

   b. How do your organization's stakeholders manage their data?

   c. Are there any unique processes / activities specific to your organization, Fusion Center, region, or stakeholders?

   d. Would these processes / activities be affected by the power outage or relocation of operations / services?

4. What Federal coordination is occurring?

   a. For local government, what assets or resources are available to assist your organization? How are information and updates communicated?

   b. For private sector owners / operators, what assets or resources are available to assist your organization? How are information and updates communicated?

5. How will your organization continue to manage response efforts while beginning long-term recovery processes?

   a. What are the implications of a long-term power outage for your sector / agency?

   b. What governmental (Federal / State / local) resources would your organization request?

Emergency Services

1. What are your organization's interdependencies?

   a. What stakeholders are dependent upon your organization and its services?

   b. Who are the key stakeholders or groups that your organization relies upon to help restore your operations and assets? What public organizations / resources does your organization rely on to help restore your assets?

   c. Who are the key mobilizers or champions (either individuals or functional roles) who must be engaged?

2. What types of information are needed to assist in restoration of your organization's critical infrastructure?

   a. What information would your organization expect to receive? How does your organization expect to receive it and from whom?

   b. What information would your organization expect to provide? How would your organization expect to provide it, and to whom?

3. What resources / services (e.g., transportation, power, water) are most critical for restoring your organization's critical infrastructure assets?
    a. Who controls / owns these resources / services?
    b. How long can your organization continue to function without these essential services?
    c. Do you have contracts / agreements in place with the organizations that control / own these resources / services needed to maintain priority services for your jurisdiction in an emergency?
4. What public sector assets or resources are needed and available to assist your organization and the overall response effort?
5. What information would be released to your customers and the general public at this point?
    a. Who would make decisions regarding release of information to the public?
    b. What organizations would produce the most useful information for public information purposes? Do you have existing relationships with these organizations?
    c. How is your organization coordinating messages with the public sector?

Government Agencies

1. If relocation of your operations / services became necessary, how would your organization coordinate with the private sector?
    a. If your organization relocates to an alternate location, what information and communication systems are in place to allow you to coordinate with critical private sector partners?
2. What private sector assets or resources are available to assist your organization and the overall response effort?
    a. Are pre-arranged agreements in place with private sector organizations to provide resources?
    b. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
    c. How will this coordination and information sharing take place?
3. What aid would your organization provide to private sector assets or resources?
    a. How are roles and responsibilities delineated?
    b. What plans or programs outline this aid or assistance?
4. What public communications or warnings is your organization disseminating?
    a. Who would make decisions regarding release of information to the public?
    b. What organizations would produce the most useful information for public information purposes? Do you have existing relationships with these organizations?
    c. How is your organization coordinating messages with the private sector?

This page is intentionally left blank.

APPENDIX A: EXERCISE PARTICIPANTS

Participating Organizations
Private Sector
[Private sector participants]
Federal
[Federal participants]
State
[State participants]
Local
[Local participants]
Other
[Insert additional participants]

This page is intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Definition
AAR	After-Action Report
C-IED	Counter-Improvised Explosive Device
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
DCS	Distributed Control System
DHS	Department of Homeland Security
EMR-ISAC	Emergency Services Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
HAZMAT	Hazardous Materials
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
INL	Idaho National Laboratory
IT	Information Technology
JIB	Joint Intelligence Bulletin
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NSI	Nationwide Suspicious Activity Reporting Initiative
NSTB	National SCADA Test Bed
NTAS	National Terrorism Advisory System
PSA	Protective Security Advisor
RAT	Remote Access Trojan
SAR	Suspicious Activity Reporting
SCADA	Supervisory Control and Data Acquisition
SitMan	Situation Manual
SME	Subject Matter Expert
TSO	Transmission System Operator
TTX	Tabletop Exercise
VBIED	Vehicle Borne Improvised Explosive Device