STANDARD SURVEY

When you only have core data elements, such as an address, in the notebook:

- The information within the Notebook is sensitive and should be safeguarded as For Official Use Only (FOUO). It should not be released to an unauthorized individual. It may enjoy some disclosure protections. Any disclosure penalties will be handled at the FOUO level. No submission identification number is needed on the Cover Sheet.

This document is not Protected Critical Infrastructure Information (PCII) until writing occurs:

- Once you start writing in this notebook, please tear off this page to reveal the PCII Cover Sheet. Thank you.

When you have answered some of the security-related questions, but not all of the parent questions (topic-initiating questions):

- PCII disclosure protections, dissemination restrictions, and safeguarding principles will apply to this information, but the assessment is still considered incomplete, and a " draft". Disclosure penalties would not be enforced. No submission identification number is needed on the Cover Sheet.
- Expiration of Incomplete Assessments Remaining On Notebook: The assessor is encouraged to manually delete incomplete or working assessments remaining in the notebook that reach a 90-day timeline, starting from the time core data elements are pre-populated into the notebook.

After online data entry is complete, or after Builder upload (with data check) is complete:

- Please **shred this notebook**. Thank you.

This page is intentionally left blank

OMB Control Number: 1670-NEW
Expiration Date: XX/XX/XXXX

Privacy Act Statement:
Authority: 44 U.S.C. § 3101 and 44 U.S.C. § 3534 authorize the collection of this information.
Purpose: DHS will use this information to create and manage your user account and grant access to the Infrastructure Protection (IP) Gateway.
Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792.
Disclosure: Furnishing this information is voluntary; however failure to provide the information requested may delay or prevent DHS from processing your access request.

Paperwork Reduction Act: The public reporting burden to complete this information collection is estimated at 7.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/NPPD/IICD, Kimberly Sass, Kimberly.sass@hq.dhs.gov ATTN: PRA [OMB Control Number 1670-New].

This page is intentionally left blank

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

N o n d i s c l o s u r e

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of 6 CFR Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and disseminated in accordance with the CII Act and the PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-assist@dhs.gov within 30 days of receipt of this information. You will receive an e-mail containing the PCII user training. Follow the instructions included in the e-mail.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and Demonstrate a valid need-to-know.
- The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

E-mail: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular e-mail channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related e-mail accounts.** Whenever the recipient forwards or disseminates PCII via e-mail, place that information in an attachment**.**

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**." Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Tracking Number(s) of the source document(s) must be included on the derivatively created document in the form of an endnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

This page is intentionally left blank

TABLE OF CONTENTS

This page is intentionally left blank

GENERAL

What is a facility?
A basic question throughout the survey will be, "What is the 'facility'." For instance:

- A tall commercial building assigned to the commercial sector is the named asset; the whole building is the facility.
- A securities transfer company, assigned to the banking and finance sector, located on Floors 13-20 of a tall commercial building, is the named asset; only Floors 13-20 are the facility, with the building access controls, if any, attributable as the perimeter controls for the facility and the building utilities as the dependencies for the securities transfer company facility.
- A BSL-4 laboratory, assigned to the public health sector and located on a college campus is the named asset; only the building housing the BSL-4 laboratory is the facility.

As a general rule, any part of the question set that talks about a plan or the area in general is assumed to be the same at the SAA's. It would be unusual to have a different security plan or business continuity plan for an SAA verses the facility. However, the sections that refer to the specific physical security (e.g., fences, gates, illumination, barriers) may be different between the facility and a given SAA. In the IST process, if there is a difference between the facility level physical security and the SAA physical security, the weaker of the processes should be selected. In the SAV, the differences can be identified by selecting the SAA and then marking the specific physical security elements related to that SAA.

One exception is that for public venues (e.g., stadiums, arenas and theaters) the survey should be completed as if it is "game day" or "event day". Since the threat to these types of facilities is due to the crowds in attendance, it is proper to complete the survey for the **weakest protective measures** for the facility when it is full of people (with a few exceptions outlined in the appropriate section). The primary focus should be the main or primary event that occurs at that facility that generates the largest crowd or most interest.

Significant Areas or Assets
Once the definition of the facility has been determined, then significant areas or assets of concern (SAAs) can be designated. For instance:

- The main lodging building in a large resort asset that covers 100s of acres.
- The HVAC system intakes, and lobby in a tall commercial building asset.
- In a BSL-4 laboratory asset, the clean room, and agent storage refrigerators.

In certain sections, if the answers apply to one or more SAAs, please so indicate in the appropriate question. If the answers are for the facility in general, do not select any specific SAAs.

The multiple selection questions throughout the IST have been arranged such that typically the weakest selection is the last selection in the list.

COMMENTS AND BRIEFING NOTES

Blank areas have been provided for general comments. Consider briefing notes internal use only and comments will be available to all external users. Comment areas are for any comments that may be useful in QA or to explain a checkbox answer more fully. Briefing note areas are for short bullets that the outbriefer can use to quickly assemble the outbriefing and should only contain something that would be outbriefed to the facility.

Facility Information	
Facility Name	_____
Other facility names/Aliases	Site Alias: _____
Visit Date(s)	**Start Date:** _____ **End Date:** _____
Who completed the IST?	☐ Resident PSA ☐ Non-resident PSA Name: _____ ☐ National Guard SAV Team Team: _____ ☐ Other (e.g., SME) Name: _____
Street Address, (City, County, State, ZIP Code, Country)	_____
Congressional District	_____
Latitude/Longitude *(Decimal format preferred.)*	Latitude**:** _____ Longitude**:** _____
Visit Motivation *(Check all that apply)*	☐ ECIP/IST ☐ SAV ☐ RRAP ☐ Facility Request ☐ Law Enforcement Request ☐ Direct Threats/Suspicious Incidents Identify: _____ ☐ Special Event Name of Event: _____ ☐ Other Identify: _____
Why is this facility important to another PSA?	*Explain:* _____
Why was this facility identified for an SAV?	*Explain:* _____
How was the interview conducted?	☐ Interview Only ☐ Partial site orientation ☐ Full site orientation

FACILITY INFORMATION

Who completed the IST?
This question captures when an IST is conducted by someone with responsibility for the facility but who is not the Resident PSA. This may occur during an RRAP or special regional/system/cluster assessment when the Resident PSA may be assisted by Non-Resident PSAs or when the IST is generated from data gathered during an SAV. In the case of an SAV, select Other.

Why is this facility important to another PSA? For an SAV, Why was this facility selected for an SAV?

These questions should be answered by the PSA for capturing the importance of this facility or critical infrastructure.

Of all the questions within the IST, this one should probably have the most thought put into it. Try to answer this question with something other than what has been filled in for site description. You can read everything about market share or purpose of the site, but what would you really need to know about this facility if you had never been there. Try to put the facility and related information in context so that a reader fully understands why you visited the site, how it fits into the region or area and why it is important, or in some cases, not so important. Provide insight and comment as to why this facility was even visited. This information will be available to all viewers of the IST and will have particular interest to a PSA from outside the area who is supporting an event or filling in for another PSA.

Good answers may address:

- Past interactions with law enforcement that causes them to think they would require special consideration during an incident or event.
- What is important, why it is important, how the facility or system interconnects to other facilities and systems, who is important to know at the faculty and if an event should occur in the region or at the facility, when does the facility or system become so important that DHS HQ needs to know about it.
- Notes if the facility has some symbolic/psychological importance (e.g., religious affiliation, political affiliation, unique personnel, or children or other high-profile occupants).

Poor answer is:

- To repeat that the facility is a large commercial building or the road / bridge carries a large amount of traffic.

Facility Information	
General Facility Description:	Describe: _____ Approximate size: _____ _____ acres **or** _____ square footage Tallest occupied structure: _____ stories **or** _____ feet
What are the operating hours of this facility?	☐ 24 / 7 / 365 ☐ 24 / 7 / closed for some days during the year ☐ 24 / less than 7 days a week ☐ Less than 24 hours a day, 7 days per week ☐ Less than 24 hours a day, less than 7 days per week ☐ Only for special events 180 days or more per year ☐ Only for special events less than 180 days per year
Are you aware of the DHS "See Something Say Something" campaign?	☐ No (If No, PSA should provide flyer or information on program) ☐ Yes (If Yes, select all that apply) ☐ Aware of program, but no action taken ☐ Aware of program, but no materials available or provided ☐ See Something Say Something materials are posted within the facility (select all that apply) ☐ Flyers ☐ Posters ☐ PA Announcements ☐ Daily, weekly or monthly email message ☐ Suspicious activity has been reported at this facility directly due to See Something Say Something campaign ☐ Employees have stated that there is a heightened sense of security awareness due to See Something Say Something campaign

General Facility Description

This section is to give a general overview of the facility. Think of how you would describe an aerial photograph or map of the facility.

- How big is the facility – total acreage or square footage
- Is it a complex or simple facility – total number of buildings or other structures – a facility with one building or a facility with 30 buildings/structures? Structures are non-buildings such as process units (e.g., storage tanks, process towers, large antenna/dishes).
- Are the buildings large or small –if there are multiple buildings, include the approximate square footage of the largest building in the square footage block and then give short descriptions and sizes of each of the main buildings with the approximate square footage.
- Is the building subject to certain types of attack – the tallest (highest) structure on the site and the deepest structure (below ground basements, but not piping)?
- Developed (e.g., buildings, parking lots) or undeveloped (e.g., no structures or paving).

Facility Information	
Are you aware of the PS-Prep™ certification program?	☐ No ☐ Yes (If Yes, select all that apply) ☐ Aware of program, but no plan to obtain certification ☐ Aware of program, and plan to obtain certification ☐ Aware of program, and have already obtained certification
Does your facility use some standard to guide your risk management activities?	☐ Do not utilize any type of standard ☐ Aware of standards, but do not currently use ☐ Aware of and use standards Which standards do you use? ☐ ISO 22301 ☐ ISO 31000 ☐ ANSI/ASIS SPC. 1-2009 ☐ NFPA 1600 ☐ BSI 25999 ☐ Other _____

In 2007, Congress directed the Department of Homeland Security (DHS) to establish and implement the voluntary private sector preparedness accreditation and certification program (PS-Prep). The result of this directive, PS-Prep™, is designed to improve the preparedness of private sector and not -profit organizations through conformance to consensus-based preparedness standards and best practices. PS-Prep™ will enable organizations to identify and implement the necessary steps for instituting and maintaining a comprehensive management system that addresses business continuity, organizational resilience, emergency and disaster management. In addition, DHS will provide recognition for those entities, which certify to the adopted preparedness standards. PS-Prep™ is a voluntary program, primarily serving as a resource for private and non-profit entities interested in instituting a comprehensive business continuity management system. Incorporating three industry standards, PS-Prep™ offers organizations the opportunity to develop and maintain certification to nationally recognized and respected approaches to resilience and preparedness.
See, http://www.fema.gov/ps-preptm-voluntary-private-sector-preparedness

ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
See, http://www.iso.org/iso/catalogue_detail?csnumber=50038

ISO 31000:2009 provides principles and generic guidelines on risk management. ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.
See, http://www.iso.org/iso/catalogue_detail?csnumber=43170

ASIS SPC. 1-2009 - Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. This management system standard has applicability in the private, not-for-profit, non-governmental and public sector environments. It is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a disruptive incident (emergency, crisis, or disaster). It enhances an organiztion's capacity to manage and survive the event, and take all appropriate actions to help ensure the organization's continued viability. The body of the document provides generic auditable criteria to establish check, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.
See, www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf

National Fire Protection Association (NFPA) 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs. This standard provides disaster and emergency management and business continuity programs, the criteria to assess current programs or to develop, implement, and maintain aspects for prevention, mitigation, preparation, response, and recovery from emergencies.
See, http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf

BSI 25999 - Business Continuity. This standard is designed to keep business going during the most challenging and unexpected circumstances protecting staff, preserving reputation and providing the ability to continue to operate and trade. This standard has been replaced by ISO22301.
See, www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/

Primary Facility Contact	
First Name	_____
Last Name	_____
Title	_____
Company / Agency	_____
Phone	Office: _____ Cell: _____ Other: _____
24 Hour Contact	_____
Email	_____

☐ Dashboard recipient
☐ Participated in site visit

Owner Operator Contact (may be different than facility POC)	
Same as Primary Facility POC ☐	
First Name	_____
Last Name	_____
Title	_____
Company / Agency	_____
Phone	Office: _____ Cell: _____ Other: _____
Email	_____

☐ Dashboard recipient
☐ Participated in site visit

Other Facility Contacts, Visit Participant , First Responders (replicate as needed)	
First Name	_____
Last Name	_____
Company / Agency	_____
Title / Position	_____
Phone	Office: _____ Cell: _____ Other: _____
Email	_____

☐ Participated in site visit

FACILITY POC AND VISIT PARTICIPANTS

Include a single facility POC. Typically this may also be the primary POC for the company and the 24 hour contact and the person that will receive the dashboard. On occasion, the facility POC will not be be the owner / operator.

Under other facility POC and visit participants, list all persons contacted during the visit or provided by the owner. This includes any first responders. If the person participated in the site visit select the box indicating participated in visit.

Facility contact that should receive primary access to the Infrastructure Survey Dashboard
Please identify the individual that will the primary user of the dashboard; if applicable, please select the individual that has signed the E&C. This user will be able to create additional users for the site. If this is an SAV, this individual will also receive the SAV report through the Infrastructure Survey Dashboard.

Other Facility Contacts, Visit Participant , First Responders
Please provide contact information concerning all people that participated to the visit as well as the first preventers/responders. For the first preventers/responders, provide at a minimum the contact information concerning Law Enforcement Agency, Fire Response Agency, and Emergency Medical Response.

Significant Area(s) and Asset(s) *(replicate as needed)*	
SAA Name/POC	**Location**
SAA Name: _____ **POC (if different from Facility):** _____ **Name:** _____ **Email:** _____ **Cell Phone:** _____ **Office Phone:** _____	**Street Address (if significantly different from Facility)** **Lat:** _____ **/ Long:** _____ **(Degrees, Mins, Secs.)**
Description/Function	**Consequence of Loss**
Type of SAA *[check Sector SAA list]* **Describe SAA:** _____ **Describe Function:** _____	If this SAA is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted (e.g., resulting in an unacceptable loss of business function): _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) If this SAA is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded: ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% If this SAA is lost, is there a backup or an alternative mode? ☐ No ☐ Yes Describe: _____ If this SAA is lost and any backup or alternative mode is employed, what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% Duration of backup: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)

SIGNIFICANT ASSET(S) AND AREA(S)

A Significant Asset / Area is:

- Something critical to operation/function of the facility
- Something critical to the physical vulnerability of the facility
- An aspect about the facility that may be important to intelligence or risk assessment analysis for this type of facility

Critical to Physical Vulnerability

- Access Protective Measures
- Avenues of Approach
- Security Presence
- Recognizability
- Drop-off points

Important Characteristic

- Areas where special events take place or people gather

A Significant Asset/Area is NOT:

- A component already captured in the Dependencies section (e.g., emergency generators or water connections)
- People or buildings while occupied. The exception is a public venue such as an NFL stadium, NASCAR track or other large public venue, such as a convention center which should be assessed as "event day" since at other times it is less attractive as a target. It is understood that many of these facilities operate year round (like a college stadium) or have many different events like arenas that host different concerts. For NFL, NASCAR, NCAA type events, select the main event. For concerts, convention centers, select the most common. For reference see HELP on Suggested Significant Assets.

HINT: If the SAA is damaged, lost, stolen, destroyed, broken, flooded, blown into another county, or is otherwise not available, not usable, or not operational and there is no discernible impact to the facility or the function of the facility, then the asset might not be an SAA.

If this SAA is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted (e.g., resulting in an unacceptable loss of business function):

This is different from the consequence of loss of a dependency (e.g., loss of electric power or water service). It is the loss of an SAA. This question captures the impact of the impact of the worst case scenario: the fact that the SAA is lost and no alternate can be used.

If this SAA is lost (without considering any backup or alternative mode), what percentage of normal business functions are lost or degraded:

This is different from the consequence of loss of a dependency (e.g., loss of electric power or water service). It is the loss of an SAA. This question captures the impact of the impact of the worst case scenario: the fact that the SAA is lost and no alternate can be used.

Significant Area(s) and Asset(s) *(replicate as needed)*	
	If this SAA is lost, how long would it take to replace the SAA and return to full operations? _____ hours (enter the number of hours) OR _____ days (enter the number of days) OR _____ months (enter the number of months) Does the facility require specialized materials, transport, and/or personnel to recover full operations? ☐ No ☐ Yes Describe*:* _____ If yes, does the facility have immediate access to such specialized materials, transport, personnel required to recover full operations? ☐ No ☐ Yes *Describe:* _____

If this SAA is lost, how long would it take to replace the SAA and return to full operations?

This is different than the consequence of loss of a dependency (e.g., loss of electric power or water service). It is the loss of an SAA. The replacement can be through the repair or reconstruction of the SAA or through the use of a temporary or permanent replacement process that provides the same capability.

Does the facility require specialized materials, transport, and/or personnel to recover full operations?

This would include such things as specialized parts such as unique transformers or pumps, specialized transport such as the large flatbed rail carriers needed for the very large transformers or barges for large equipment, and specialized teams over and above normal employee. Some key elements include extremely long lead time (3-6 months), or unique manufacturing that requires extensive design or it is a "one of" type part that is made to order on demand. If something has to be ordered and will be on the delivery truck and on its way the next day that is typically not the specialized material that is intended. It is understood that almost every sector has some specialized equipment, but the key element here is the delivery, manufacture, and time to install is of such extensive time and effort that there is a business impact that is challenging to respond to. In isolated cases there are only select individuals or teams of people that can fix or repair a particular "thing". Again the key element is long lead time, special skill or a skill that is very rare. "Calling the repair guy" or contracting the IT person is normally not considered specialized personnel for this definition.

If yes, does the facility have immediate access to such specialized materials, transport, personnel required to recover full operations?

The facility has spare parts close, onsite, or within 24 hours. If specialized transport is required it is immediately available and in full control of the facility.

First Preventers/Responders Interaction (only primary agency required)	
Law Enforcement Agency	_____
Service provided by Agency or supporting agency (Check all that apply):	☐ **Law Enforcement** ☐ **SWAT or Tactical Team** ☐ **Bomb Squad** ☐ **Maritime support** ☐ **Air support** ☐ **Other:** *Describe:* _____
Is there a written MOU/MOA with this first responder [not just 911]?	☐ No ☐ Yes
Have there been onsite visit(s) with this first responder?	☐ No ☐ Yes
Is there Interoperable Communication with this first responder [not 911]?	☐ No ☐ Yes Describe: _____

FIRST PREVENTERS/RESPONDERS

The questions for First Preventers/Responders are asked for each agency listed. Information concerning offsite capabilities **must be collected for the following**:

- Primary Law enforcement Agency,
- Primary Fire Response Agency, and
- Primary Emergency medical Response Agency.

The intent here is to capture the public-private partnership between the facility and first responders such as if the first responders are familiar with facility configuration and processes. As mentioned in the BCI Good Practice Guidelines (2010), an organization should be familiar with the procedures of the local emergency responders, and contact with these groups in advance may provide useful information to assist in selecting tactical options.

If you want to provide further information concerning other first preventers/responders agencies, please use the comments or briefing notes boxes.

First Preventers/Responders Interaction with Facility

Is there a written MOU/MOA with this first responder [not just 911]?
This should be a special agreement that the facility has with first responders, not just dialing 911 or a verbal agreement to drive by on a regular basis. In order to check that the facility has MOA or MOU with law enforcement, the facility must have an agreement that the law enforcement agency will supply special services to the facility in the event of a threat, attack or incident. It does not mean that the law enforcement agency will answer a 9-1-1 call in the normal course of business. For example, under an MOA/MOU, the local law enforcement would send police officers to guard the facility in the face of a specific threat or an MOA/MOU to park a police car at the facility during special events.

Have there been onsite visit(s) with this first responder?
Note that if the facility has specific training or exercises with first responders, this information should be captured in the preparedness section under business continuity and emergency action procedures.

Is there Interoperable Communication with with this first responder [not 911]?
Interoperable communications is the ability of emergency responders to work seamlessly with other systems or products without any special effort, including capability communications equipment and bandwidth. Interoperable communications is a common platform for interoperability among sheriff's offices, local law enforcement, health departments, EMA/Homeland Security, fire/EMS agencies, hospitals and other agencies having the capability of accessing the system (e.g., MARCS).

Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized. For example, when communications systems are interoperable, police and firefighters responding to a routine incident can talk to each other to coordinate efforts.

First Preventers/Responders Interaction (only primary agency required)	
Fire Response Agency	_____
Service provided by Agency or supporting agency [Check all that apply]:	☐ **Fire Response** ☐ **Hazardous Materials Response** ☐ **Maritime fire support** ☐ **Airborne fire support** ☐ **Other:** *Describe:* _____
Is there a written MOU/MOA with this first responder [not just 911]?	☐ No ☐ Yes
Have there been onsite visit(s) with this first responder?	☐ No ☐ Yes
Is there Interoperable Communication with this first responder [not 911]?	☐ No ☐ Yes Describe: _____

First Preventers/Responders Interaction (only primary agency / company required)	
Emergency Medical Response	_____
Service provided by Agency or supporting agency [Check all that apply]:	☐ **Emergency Medical Response** ☐ **Hazardous Materials Response** ☐ **Maritime medical response** ☐ **Air Evac medical response** ☐ **Other:** *Describe:* _____
Is there a written MOU/MOA with this first responder [not just 911]?	☐ No ☐ Yes
Have there been onsite visit(s) with this first responder?	☐ No ☐ Yes
Is there Interoperable Communication with this first responder [not 911]?	☐ No ☐ Yes Describe: _____
First Responder Briefing Notes: _____	
Overall First Responder Overall Comments: _____	

Consequences	
What is the function of this facility (e.g., produces, sells, stores, or transfers)?	Purpose: _____ Key Products/Services: _____
Is the facility a lifeline critical infrastructure (e.g., a utility provider/asset)?	☐ No ☐ Yes *Describe:* _____
Who is the primary customer/user of this facility's product or service?	*Describe*: _____
Is this facility the only supplier of products or services for this customer? **If not the only supplier, does this facility hold a large market share for its products or services in the region or nation (e.g., over 33%)?**	☐ No ☐ Yes *Explain:* _____ ☐ No ☐ Yes *Explain:* _____
Can other competitors or similar sister companies/facilities provide the product or service without major price impacts or delivery delays?	☐ No ☐ Yes If yes, explain: _____

CONSEQUENCES

Answers to most of the questions in this section are prepopulated. However, you have the ability to change this information if you think it is not accurate. If you decide to overwrite the information provided, please justify your decision with an appropriate explanation in the description text boxes.

Is the facility a lifeline Critical Infrastructure (e.g., a utility provider/asset)?
A lifeline Critical Infrastructure is a facility that provides an essential service to the population. These include the basic utilities of electric, gas, water, and wastewater. Outside of those sectors there are only rare and isolated incidents where something will be considered a lifeline critical infrastructure in this methodology.

Can other competitors or similar sister companies/facilities provide the product or service without major price impacts or delivery delays?
These questions are to determine the cascading impacts of the loss of this facility (criticality). If the facility has a sole-source contract with its customer(s) (i.e., at this time the customer does not receive the product or service from anyone other than this facility), the loss of the facility will impact the customer. If other competitors or similar companies can provide the product or service, then even if the facility is lost, the customer could continue to receive the product or service. This could be another facility within the same corporate owner or a competitor's facility. However, the customer may experience a price impact (e.g., the facility was the lowest bidder in supplying chlorine to a City utility) or delivery delays (e.g., a new contract must be negotiated with the competitor before deliveries may commence). For public service facilities such as police stations, courthouses, EOCs, etc., the determination is more difficult. Just because a county courthouse is the only facility in that county, in most cases another county nearby could assist and pick up the load or assist in some way until the facility or organization could become operational.

Market share is the percentage of the total available market for the product or service supplied by the facility. It can be expressed as a company's sales revenue compared to total nationwide sales revenues for the same product/service or in units of volume produced by the facility divided by the total volume of units sold in that market. For instance, there are only two US manufacturers of hydrogen fluoride. If there are only two plants, each plant would have a 50% market share. Please note: these answers are for the facility being visited, not the entire owner corporation or entity. So, if a company has 50% of hydrogen fluoride in the country, but the facility is one of five plants, it only has some lesser percentage of the market (e.g., 10%) and the answer would be no, the facility itself does not hold a large market share. For public service facilities such as police stations, courthouses, EOCs, etc., market share is simply not required, so the best response is "No.".

For profit companies usually know if they have a large market share (e.g., over 33%) even if not the exact percentage. However, certain facilities, particularly those in the public service sector, where this is a difficult question. For instance, a bridge does not have sales revenue; however, it may have volume of regional traffic. If the bridge handles 50% of the traffic across the bay to San Francisco, then this is a large market share. Also, in the public service sector, just because the water district is the sole source of water to its customers, an individual water treatment plant may only serve some portion of that market share. The answer should almost always be "No" for a stadium, arena, convention center, school, church or similar facility. There are very few of these in the Nation that have a large market share.

Consequences	
Maximum facility population at any one time (include special events, employees, contractors and visitors)	Approximate Number (a single value with no text): _____ *Describe:* _____
Is the facility considered a Chemical, Biological, Radiological, Nuclear, or Explosive facility	☐ No ☐ Yes *Describe:* _____
Maximum offsite population that will be impacted by a reasonable worst case scenario at the facility (human impact such as death or injury, not economic impact)	Approximate Number (a single value with no text): _____ *Describe:* _____
Would an incident at the facility cause an immediate mass evacuation of the facility and a large population (over 20,000 people) within the surrounding area?	☐ No ☐ Yes *Describe:* _____
Is the facility located in a DHS UASI city? (or metropolitan statistical area)	☐ No ☐ Yes
Is the facility part of a designated system (e.g., electric grid, pipeline, railroad, or mass transit system)?	☐ No ☐ Yes *Describe*: _____

Maximum facility population at any one time
This is the most important population number for the template. The intent of the question is to estimate the largest potential population at a facility or node within a system at any one time. To some extent, this is an attempt to estimate the potential loss of life should an attack occur at that location. For some types of facilities, this is not easily determined, but if you just think of loss of life during an attack it may be easier. The intent is to provide some reference to the maximum potential impact to population knowing that in almost all cases the final number of people impacted will likely (and hopefully) be significantly smaller. For instance:

- For a bridge you may know the number of cars that traverse the bridge every day; however that is not the maximum population at any one time. So, you may have to be creative and determine the maximum number of cars that could be on the bridge at any one time and multiply by the estimated number of people per car and add that to the maximum number of pedestrians that could be on the bridge to get that potential loss of life population number.
- For a stadium, obviously, it would be the maximum capacity during an event and also consider the people in the parking lots tailgating. We understand that in most cases a stadium or bridge or most other facilities and all occupants and visitors to that location will not be immediately and totally removed from the face of the earth.
- For transportation, a good answer will identify the maximum capacity of a commuter rail train at a busy stop, or, the typical maximum attendance at the Indianapolis 500, or the busiest location or meeting area of a parade route or a shopping mall. A poor answer will identify car count on a highway overpass with no reference to time.

Is the facility considered a Chemical, Biological, Radiological, Nuclear, or Explosive facility? For chemical, under the authority of section 112(r) of the Clean Air Act, the Chemical Accident Prevention Provisions require facilities that produce, handle, process, distribute, or store certain chemicals to develop a Risk Management Program, prepare a Risk Management Plan (RMP), and submit the RMP to EPA. The offsite consequences analysis of the RMP identifies the potential reach and effect of hypothetical worst-case accidental releases from the facility for each regulated chemical. It is reasonable to ask a facility if they are subject to and have an RMP. Biological would, for instance, include any of the Biological Safety Laboratories (e.g., BSL-3) certificated by the National Institutes of Health or equivalent. Radiological would include any facilities that have sufficient radiological sources to require licensing by the Nuclear Regulatory Commission (NRC) and can include hospitals and nuclear reactors (commercial or experimental). Explosive would include any facility that would have to comply with Occupational Safety & Health Administration (OSHA) regulations for explosives and blasting agents or Department of Transportation placarding requirements. CBRNE may not be a term a private sector recognizes or utilizes, but the concept is the same. You are trying to determine if the facility has elements onsite that could be weaponized or stolen thus making that facility more likely to be targeted or may cause harm through accidental release.

Maximum offsite population that will be impacted by a reasonable worst-case scenario at the facility [death and injury, not economic impact]
While this is related to maximum population, it is more subjective and is an attempt to capture the human impact of the worst-case incident at the facility. As an example, a small chemical manufacturing facility with high quantity of TIH, 50 employees in a rural area and no other population within 20 miles, the impact would be the employees, thus 50. The same company in an urban area, with a nearby population of 15,000 within the offsite consequence calculation, the input value would be 15,000. The intent is that the unfavorable event must occur at the facility and then create an offsite impact. If everything is confined to the facility the entry for Maximum facility population at any one time meets the intent. Thus it is possible that the response to the offsite question may be answered as zero.

Consequences	
Would an incident at the facility cause an immediate mass evacuation of the facility and a large population (over 20,000 people) within the surrounding area?	☐ No ☐ Yes *Describe:* _____
Is the facility located in a DHS UASI city? (or metropolitan statistical area)	☐ No ☐ Yes
Is the facility part of a designated system (e.g., electric grid, pipeline, railroad, or mass transit system)?	☐ No ☐ Yes *Describe*: _____

Would an incident at the facility cause an immediate mass evacuation of a large population (over 20,000 people) within the surrounding area?
An **immediate** mass evacuation of over 20,000 people must have been caused by the incident at the facility. The evacuation must be immediate, not that over time the loss of water, wastewater or electric service would cause the eventual evacuation of an area (e.g., due to health concerns or convenience of the population). There are very few facilities that have materials or processes on site that will cause an immediate evacuation. A refinery, chemical plant, large water park with chlorine, a CDC-certified Biosafety Level Laboratory (BSL) or nuclear facility may be some examples if they are located near populate areas.

Is the facility located in a DHS UASI city?
Check against latest UASI City list. Only looking for current, not included if it was a UASI in the past.

Is the facility part of a designated system (e.g., electric grid, pipeline, railroad, or mass transit system)?
This could include anything like electric substations, generating plants and control rooms; water treatment plants, pump houses and surface water intakes; public transport stations, switch houses, control rooms, and rolling stock; wastewater treatment plants, pump houses, outfalls; or natural gas pipeline segments, compressor stations, controls rooms and treatment plants.

Consequences	
Civil Government Impact **Would there be a discernible civil government impact due to the loss of the facility or its operations?**	☐ No ☐ Yes
Asset Replacement Value:	*Give an approximate dollar amount and explanation.* ☐ $ 500,000,001 or greater ☐ $ 100,000,001 to 500,000,000 ☐ $ 20,000,001 to 100,000,000 ☐ $ 5,000,001 to 20,000,000 ☐ Less than $5,000,000 *Describe:* _____
Business Interruption	*Give an approximate dollar amount and explanation.* ☐ $ 1,000,000,001 or greater ☐ $ 500,000,001 to 1,000,000,000 ☐ $ 100,000,001 to 500,000,000 ☐ $ 10,000,001 to 100,000,000 ☐ Less than $10,000,000 *Describe:* _____
Consequences Briefing Notes: _____	
Overall Consequences Comments: _____	

Civil Government Impact
The type of information to include here is not just that loss of life or injuries from an event at the facility would overcome any hospital in the area; it should be that the facility supplies something that is necessary for emergency response or provides some product or service needed for these activities – more of a cascading effect from loss of the facility operations/output. For example, the loss of a telecom hotel shuts down the city-wide 911 system. The loss of a state capitol complex would have an impact to the operation of the state government through loss of records, the ability to distribute welfare checks, or to the ability of the state legislature to pass emergency bills and funding resolutions in the time of emergency.

Asset Replacement Value:
Asset replacement costs apply to site equipment, units, or other onsite property damaged beyond repair that would need to be replaced to restore the original functionality of the equipment or units to its design productivity levels. This value is estimated whether the owner plans to rebuild or not. The adversarial attack scenario which yields the highest damage should be used as the basis for the estimate.

Here are examples of the construction values for different assets:

- $ 500,000,001 or greater:
  One World Trade Center (3800 million in 2013), Yankee Stadium: (1560 million in 2009), Trump Tower Chicago (847 million in 2009), Soldier Field (800 million in 2003), and Marlins Park (634 million in 2012)
- $ 100,000,001 to 500,000,000:
  Pat Tillman Bridge in NV near Grand Canyon (240 million in 2010), I35 new bridge to replace one that fell (230 million in 2007)
- $ 20,000,001 to 100,000,000:
  8-24 story Hotel (60 million in 2008), 4-8 story Hospital (50 million in 2008), 11-20 story office building (35 million in 2008)
- $ 5,000,001 to 20,000,000:
  High school (18 million in 2008), 1-2 story courthouse (11 million in 2008)
- Less than $5,000,000:
  2 story Fire Station (2 million in 2008), Gas station (1 million)

These values must be used only as indicators.

You can find more information on the following link:
http://www.reedconstructiondata.com/rsmeans/models/

Business Interruption
Business Interruption costs include the total loss of sales or income for a 12-month period.

Natural Hazards	
Is the facility located in an area that experiences any of the following natural hazards? **Check all that apply**	☐ Hurricane Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____ ☐ Flood Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____

NATURAL HAZARDS

Is the facility located in an area that experiences any of the following natural hazards?
This initial question is to determine if the event occurs in the area. For example, in the State of Iowa, Severe Winter Storm, Tornadoes, should be selected for almost every facility. Flood depends on specific location within a flood plain and will be more facility specific. The impact of such events is captured in another question.

The answer to this initial question is prepopulated. However, you have the possibility to change this information if you think the information provided is not accurate. Remember that the selection or not-selection should be done regardless of previous or current impact. If you decide to overwrite the information provided, please justify your decision with an appropriate explanation in the Natural Hazards Briefing Notes.

Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard?
Constructed, modified or retrofitted to mitigate the impact of a natural hazard would require that the facility has purposefully built thefacility/asset or installed or upgraded/retrofitted the facility/asset to mitigate the impact of the natural hazard. This could include things like permanent flood walls or dikes, specially reinforced roofs for hurricanes, special earthquake resistant design and construction or raised platforms for critical equipment to prevent flood damage. This type of construction, modification or retrofitting may have been done to meet updated building standards put into place to mitigate this specific natural hazard (e.g., California building codes for strengthened building construction pertaining to earthquakes or Florida building codes for hurricanes) or may be over and above code requirements based on facility-specific hazard considerations.

Does the facility have specific plan/procedures for long term mitigation measures concerning this hazard?
The facility may have plans or procedures to mitigate the effects of a natural hazard for the long-term (e.g., hurricane season). This might include putting up snow fences for the winterstorm season or staging equipment for fire suppression during wildfire season. This could also include temporary sump pumps for critical areas, or sand/salt/snow removal equipment for winter storm response.

Does the facility have deployable mitigation measures for this specific hazard?
Deployable mitigation measures are measures that are not permanent, but can be put into place in anticipation of a specific natural hazard to mitigate the effects. These could be deployable sandbags, things like safe shut down of electric equipment before a hurricane or flood occurs to minimize damage, procedures to move equipment (e.g., rail cars or tanker trucks) out of the area, or emptying tanks of hazardous materials before a wildfire reaches the facility. In evaluating this question, only mark “Yes” if the deployable mitigation measures are effective – five sandbags vs. a process for filling and deploying a sufficient number of sandbags to protect critical areas and assets.

Natural Hazards	
Is the facility located in an area that experiences any of the following natural hazards? **Check all that apply**	☐ Earthquake Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____ ☐ Tornado Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____

Natural Hazards	
Is the facility located in an area that experiences any of the following natural hazards? **Check all that apply**	☐ Wildfire Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____ ☐ Severe winter storms (snow/ice) Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____

Natural Hazards	
Is the facility located in an area that experiences any of the following natural hazards? **Check all that apply**	☐ Lightning strikes Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____ ☐ High winds not associated with hurricanes/tornados Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____

Natural Hazards	
Is the facility located in an area that experiences any of the following natural hazards? **Check all that apply**	☐ Other natural hazard: _____ Has the facility been constructed/modified/retrofitted to mitigate impact of this natural hazard? ☐ No ☐ Yes *Describe:* _____ Does the facility have specific plan/procedures for long term and immediate mitigation measures concerning this hazard? ☐ No ☐ Yes *Describe*: _____ Does the facility have deployable mitigation measures for this specific hazard? ☐ No ☐ Yes *Describe*: _____

Natural Hazards		
Has a natural disaster ever caused an interruption to facility operations (e.g., resulting in an unacceptable loss of business function)? ☐ No ☐ Yes (If *yes check all that apply)*		
☐ Hurricane	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Flood	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Earthquake	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Tornado:	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____

Has a natural disaster ever caused an interruption to facility operations (e.g. resulting in an unacceptable loss of business function)?

An unacceptable loss of business function may vary from facility to facility. It could be that a 75% reduction in production is acceptable to a facility during a natural disaster because there is no one that needs that service until after recovery is completed (e.g., pool cleaning service). However, it might be that a 10% reduction in production is unacceptable to a facility because it is a vital service or may become even more important during a natural disaster (e.g., chlorine for water treatment or the manufacturer of firefighting foam during wildfire season).

Natural Hazards		
☐ Wildfire	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Severe Winter Storms (snow/ice)	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Lightning strikes	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ High winds not associated with hurricane or tornado	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
☐ Other Natural hazard – As described above	The last incident that caused a business interruption occurred: ☐ less than1 year ago ☐ 1-5 years ago ☐ More than 5 years ago	Estimate the duration of business interruption following the last incident: ☐ 24 hours or less ☐ 25-72 hours ☐ 3-30 days ☐ 31-179 days ☐ Greater than 180 days *Describe:* _____
Natural Hazards Briefing Notes: _____		
Overall Natural Hazards Comments: _____		

This page is intentionally left blank

Information Sharing		
Are you aware of any of the following agencies with which you can exchange information? (check all that apply)	**Federal**	**State/Local**
	☐ **FBI** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **Other Federal Law Enforcement (FPS, TSA, ICE, etc.)** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **JTTF** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information	☐ **Fusion Center** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **State CIP Coordinator** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **State Homeland Security Advisor** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information

INFORMATION SHARING

Are you aware of any of the following agencies with which you can exchange information? (check all that apply)

For each of the agencies selected, indicate if you exchange hazard and threat information. “Exchange” can mean “receive from,” “provide to,” or both. Then characterize the information received.

It is possible that no information is either provided by the facility or shared with the facility from another organization.

ATAC: Ant-Terrorism Advisor Council
ATF: Bureau of Alcohol, Tobacco, Firearms and Explosives
CDC: Centers for Disease Control
CIP: Critical Infrastructure Protection
DHS: Department of Homeland Security
FPS: Federal Protective Service
EMA: Emergency Management Agency
FBI: Federal Bureau of Investigation
HSIN: Homeland Security Information Network
ICE: Immigration and Customs Enforcement
InfraGard: FBI program for public / private partnership
ISAC: Information Sharing Analysis Center
JTTF: Joint Terrorism Task Force (or equivalent in some areas)
NOAA: National Oceanic and Atmospheric Administration
TSA: Transportation Security Administration
USGS: United States Geological Survey

Information Sharing		
Are you aware of any of the following agencies with which you can exchange information? (check all that apply) **For each of the agencies selected, indicate if you receive or provide hazard or threat information, then characterize the information received.**	**Federal**	**State/Local**
	☐ **ATF** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **ISAC (Section:_____)** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **HSIN portal** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information	☐ **State EMA** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **State Law Enforcement** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **Local EMA** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information

Information Sharing		
Are you aware of any of the following agencies with which you can exchange information? (check all that apply) **For each of the agencies selected, indicate if you receive or provide hazard or threat information, then characterize the information received.**	**Federal**	**State/Local**
	☐ **InfraGard** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **US Attorney's Office ATAC** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **DHS (Agency:_____)** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information	☐ **Local Law Enforcement** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **Industry Group** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **Public Health** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information

Information Sharing		
Are you aware of any of the following agencies with which you can exchange information? (check all that apply) **For each of the agencies selected, indicate if you receive or provide hazard or threat information, then characterize the information received.**	**Federal**	**State/Local**
	☐ **NOAA** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **USGS** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **CDC** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information	☐ **Corporate Law Enforcement or security** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ **Other** _____ ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ None

Information Sharing		
	Federal	**State/Local**
Are you aware of any of the following agencies with which you can exchange information? (check all that apply) **For each of the agencies selected, indicate if you receive or provide hazard or threat information, then characterize the information received.**	☐ **Other _____** ☐ Facility has not exchanged information ☐ Facility has exchanged information ☐ Facility has received information ☐ Information received is accurate ☐ Information received is timely ☐ Information received is relevant ☐ None of the Above ☐ Facility has provided information ☐ None	

Information Sharing	
Is there a written MOU/MOA with entities other than emergency responders (e.g., neighboring facilities, other companies, contract response companies, water and wastewater agency response networks)?	☐ No ☐ Yes Have the written MOU/MOA's with other entities been previously activated (either as an exercise or during a real incident)? ☐ No ☐ Yes If yes, Following the activation was an after action report completed? ☐ No ☐ Yes
Does any employee have a national security clearance?	☐ No ☐ Yes If yes, ☐ Corporate level ☐ Facility level
Information Sharing Briefing Notes: _____	
Overall Information Sharing Comments: _____	

Is there a written MOU/MOA with entities other than emergency responders (e.g., neighboring facilities, other companies, contract response companies, water and wastewater agency response networks)?
This is different than the MOU/MOA with emergency responders and may include Mutual Aid Agreements with neighboring facilities, contract chemical response companies, or private cleanup contractors.

Does any employee have a national security clearance?
This means that is related to the facility's security. It does not include employees that may have security for other purposes (e.g., they are National Guard members with clearance to use in that position, but not for the facility being assessed).

<table>
<tr><th colspan="3">Security Activity History and Background</th></tr>
<tr><td>Prior Vulnerability Assessments Conducted?</td><td colspan="2">☐ No
☐ Yes

If yes, Assessment Type: (Check all that apply)
☐ Industry-approved
☐ Government Agency/Regulatory
☐ Contract
☐ LLEA
☐ Internal

Assessment Date(s):
VA Type _____ Date conducted _____ Follow-up VA Date _____
_____ _____ _____
_____ _____ _____
_____ _____ _____

Is the VA shared with DHS?
☐ No ☐ Yes</td></tr>
<tr><td>Have any new protective/resilience measures or enhancements been put into place within the past year?</td><td colspan="2">☐ No
☐ Yes</td></tr>
<tr><td rowspan="11">If yes, what new protective/resilience measures or enhancements have been put in place within the past year?</td><td>Type of protective measure
(Check all that apply)</td><td>In response to a Vulnerability Assessment recommendation or regulatory/mandatory standard?</td></tr>
<tr><td>☐ Access control</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Barriers</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Communications and notification</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Cybersecurity</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Infrastructure upgrades/redundancy</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Incident response</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Monitoring and surveillance detection</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Personnel</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Planning and preparedness</td><td>☐ No ☐ Yes</td></tr>
<tr><td>☐ Security force</td><td>☐ No ☐ Yes</td></tr>
<tr><td colspan="3">New Protective Measures Briefing Notes: _____</td></tr>
</table>

SECURITY ACTIVITY HISTORY AND BACKGROUND

New Protective/Resilience Measures must be completed; items such as starting to create a plan, submitting requests, reviewing documentation are all good things, but only represent planned activities or projects underway.

New Protective/Resilience Measures must be permanent changes in procedures, policies, equipment or personnel, e.g., new cameras, developed a security plan, conducted an exercise, hired additional security force, conducted an internal assessment or cleaned out the clear zone.

If yes, what new protective/resilience measures or enhancements have been put in place within the past year?
This question is used for the calculation of both PMI and RMI.

In response to a Vulnerability Assessment recommendation or regulatory/mandatory standard?
Check yes only if the protective/resilience measures put into place in the last year in the indicated category were done in response to a written, formal vulnerability assessment (not just some agreement among the security heads that it would be a good idea) or in response to a regulatory requirement or mandatory industry standard (e.g., NERC CIP requirements for protection of cyber assets or changes required by companies that belong to the Petroleum Association, New York Stock Exchange requirement for developing, maintaining, reviewing, and updating business continuity and contingency plans (NYSE rule 446)).

Security Activity History and Background	
Does the facility security plan utilize different threat levels? ☐ **No** ☐ **Yes**	☐ DHS National Threat Advisory System (NTAS) ☐ Maritime Security (MARSEC) ☐ Industry ☐ Reflects NTAS ☐ Other: _____ *Describe:* _____
If yes, are different protective measures employed/ implemented during elevated threat situations? ☐ **No** ☐**Yes** *(If yes, check all that apply)*	☐ Additional access control ☐ Restrict access to essential personnel only ☐ Conduct inspections/searches ☐ Decrease the number of personnel authorized to be onsite ☐ Prevent onsite access by visitors ☐ Prevent parking onsite ☐ Minimize the number of gates in use ☐ Require visitor escorts ☐ Employ or enforce parking restrictions ☐ Additional barriers ☐ Add barriers at facility access points ☐ Add barriers at significant assets ☐ Increased communications and notification ☐ Lock-down control or operation centers ☐ Establish real-time communication between security and decision-level executives ☐ Coordinate security efforts with local responders ☐ Coordinate security efforts with State responders ☐ Coordinate security efforts with Federal responders ☐ Enhanced cybersecurity ☐ Additional infrastructure upgrades/redundancy ☐ Enhanced incident response (e.g., initiated MOU with Local Law Enforcement or Fire Department)

If the facility recognizes elevated threat levels, are different protective measures employed/ implemented during elevated threat situations?

Enhanced cybersecurity
This can be anything from sending out additional reminders on cybersecurity and password protections to shutting down websites or remote access portals.

Additional infrastructure upgrades/redundancy
This could be anything from bringing in additional emergency generators or portable lights to securing additional water storage or supplies.

Enhanced incident response (e.g., initiated MOU with Local Law Enforcement or Fire Department)
This could be anything from implementing an existing MOU with local law enforcement or fire department for extra services to activating a facility EOC.

Security Activity History and Background	
	☐ Additional monitoring and surveillance detection ☐ Perimeter patrols ☐ Increase frequency ☐ Increase to continuous ☐ Security Force Staffing ☐ Increase security force staffing ☐ Maximize security force staffing ☐ Increased vehicle inspections ☐ 100% ☐ Random ☐ Increased personnel inspections ☐ 100% ☐ Random ☐ Hire/contract for additional security force ☐ Provide additional illumination for remote areas ☐ Add counter surveillance teams ☐ Distribute night vision devices to security personnel ☐ Initiate Planning and preparedness ☐ Pre-assign Personnel (on-call) ☐ Assign emergency response personnel to pre-planned positions/roles ☐ Prepare to execute contingency procedures ☐ Execute contingency procedures ☐ None of the above
Protective Measures during Elevated Threat Briefing Notes: _____	
Given the opportunity what is the next security measure that the facility would like to put in place?	*Describe:* _____
To date, what is the best security investment the facility has installed/implemented?	*Describe:* _____
What best practices does the facility recommend to your peers?	*Describe:* _____
Has the facility found any security measures/practices that it would have liked to implement/install and were prohibited by regulation/ordinance?	*Describe:* _____
Overall Security Activity History and Background Comments: _____	

Additional monitoring and surveillance detection

Perimeter Controls: Increase frequency/Increase to continuous
If there were no perimeter controls previously, any new controls would be an increase in frequency. In addition, if they were once a day, increasing them to twice a day is an increase in frequency. Continuous patrols would be a team or individuals whose sole mission is a continuous ongoing patrol of the perimeter where at any given time over 75% of the perimeter is under observation.

Facility Security Force Staffing: Increase staffing/ Maximize staffing
This applies to a facility that already has a security force staff. Maximizing staff would be to cover all entry points, all SAAs, and the facility perimeter. Increasing staffing can be any increase in staffing due to the elevated threat, even just one extra guard.

Hire/contract for additional security force
This is if the facility did not previously have a security force and would either hire or contract for one.

Add counter surveillance teams
This is going to be very unusual and rare. It will occur most often related to special events and high profile events or as part of a plan during an increased threat level. This does not refer or include security guards that may have training in surveillance detection. This question is designed to capture a specialized, dedicated team or individuals assigned and trained as a duty to perform counter surveillance.

Initiate planning and preparedness

Prepare to execute contingency procedures/Execute contingency procedures
Preparing to execute contingency procedures could be sending reminders to responsible employees or distributing procedures to employees. Executing the contingency procedures would be to actually activate response teams, activate the facility EOC, and implement procedures under the appropriate plan.

Has the facility found any security measures/practices that it would have liked to implement/install and were prohibited by regulation/ordinance?
The intent is to identify possible areas of opportunity for DHS to work with eth public sector or other sectors to improve situations where a security improvement may be in conflict with a code, law, zoning issue or other restriction.

Security Management Profile	
Security Department	Is there a manager/department in charge of security management? ☐ No ☐ Yes Iif yes, is this the primary function of that manager/department? ☐ No ☐ Yes
Security Department Briefing Notes: _____	
Does the facility have a written security plan?	☐ No ☐ Yes *If yes,* The plan is developed at the: ☐ Corporate-level ☐ Facility-level Has the plan been approved by senior management? ☐ No ☐ Yes Is the plan required by a Federal, state, or local regulation? ☐ No ☐ Yes Has the plan been coordinated with local law enforcement? ☐ No ☐ Yes If yes, Is it reviewed annually with local law enforcement? ☐ No ☐ Yes Are key personnel aware of and do they have access to a copy of the plan? ☐ No ☐ Yes

SECURITY MANAGEMENT PROFILE

Does the facility have a written Security Plan?

Normally, security planning includes those things that involve security issues, such as active shooter, terrorism, hostage taking, or assassination.

The plan is developed at the: Corporate-level or Facility-level
Facility-level may include a corporate-level plan with an appendix or section for the facility being assessed that addresses the special plan provisions or procedures as they apply to that facility. If it is just a general plan that does not specifically address the facility being assessed, then select corporate-level.

Security Management Profile	
Does the facility have a written security plan?	Are personnel trained on the plan? ☐ No ☐ Yes If yes, ☐ Key personnel only are trained on the plan *(Check all that apply*) ☐ At initial employment ☐ At least once a year OR ☐ All personnel are trained on the plan (*Check all that apply*) ☐ At initial employment ☐ At least once year
	Is the plan exercised at least once a year? ☐ No ☐ Yes If yes, these exercises are: ☐Tabletop (practical or simulated exercise) ☐Includes external responders ☐Functional (walk-through or specialized exercise) ☐ Includes external responders ☐ Full scale (simulated or actual event) ☐ Includes external responders Are exercise results documented, approved and reported to executive management? ☐ No ☐ Yes

This page is intentionally left blank

Security Management Profile	
	The security plan has procedures for *(check all that apply)*: ☐ Assessment of possible security risks ☐ Review of threats to and vulnerability of facility operations/activities ☐ An up-to-date point of contact roster for: ☐ Key personnel responsible for security (e.g., Security Manager or designated representative) ☐ First Responders ☐ Identification of critical assets or areas ☐ Physical security ☐ Management and utilization of physical security systems ☐ Perimeter security ☐ Parking / delivery / standoff ☐ Electronic security systems ☐ Locks and technologies ☐ CCTV system ☐ Intrusion detection or alarm system ☐ Illumination ☐ Key control program ☐ Physical security inspection program ☐ Security force ☐ Staffing ☐ Static posts ☐ Roving patrols ☐ Equipment ☐ Training ☐ Access control Procedures ☐ Employees ☐ Visitors ☐ Contractors ☐ Customers ☐ Security awareness training program ☐ Terrorist incidents ☐ Active shooter ☐ Internal disturbances (e.g., workplace violence) ☐ Security communications policy or procedures ☐ Information protection/Operations Security (OPSEC) ☐ Personnel security ☐ Criminal activities (e.g., break-ins) ☐ Hostage situations ☐ Liaison with response agencies ☐ Exercising the plan

The security plan has procedures for (check all that apply):

Identification of pertinent risks
The plan has a discussion of pertinent risks addressed in the plan; these could include natural hazards such as hurricanes or man-made events such as cyber attacks or an irate employee/customer.

Review of threats to and vulnerability of facility operations/activities
The plan should identify pertinent threats and the gaps in security related to such threats to determine the vulnerability of the facility.

Identification of critical assets or areas
The plan should identify what areas or assets require additional security to ensure the facility continues to operate and its employees and customers are safe. These may or may not match the facility SAAs.

Exercising the plan
This section outlines how essential equipment or a process is tested, how employees and key personnel are trained and / or evaluated on the plan and the regimen for exercising the plan.

Security Management Profile	
	☐ Plan maintenance (e.g., review and revision) ☐ Executive Protection (if applicable) ☐ None of the Above
Does the facility have procedures for suspicious packages	☐ No ☐ Yes
Characterize security information communication	Does the facility notify or communicate security information to personnel? ☐ No ☐ Yes *If yes, what type of information? (Check all that apply)* ☐ Specific security incident information ☐ Recurring security awareness meetings *Describe:* _____ How does the employee report a security concern? ☐ Call-in number ☐ Phone / Radio call to security operations ☐ Phone / Radio call to security guard ☐ 911 ☐ No reporting
Does the facility participate in any security working groups?	☐ No ☐ Yes *If yes,* ☐ Federal-level security working group (e.g., InfraGard, Sector Coordinating Committee) ☐ State-level security working group (e.g., Fusion Center) ☐ Local-level security working group ☐ Private Sector /Industry security working group *Describe*: _____
Security Plan Briefing Notes: _____	

Executive Protection (if applicable)
Since this is a security management question, even if there are no key organization (corporate) executives located at the facility, the corporation may have an executive protection program, which would cover an executive should he or she visit the particular facility being assessed. If that is the case, check the box. Executive protection is when the facility security force provides personal protection for any VIP, including corporate executives or prominent visitors or performers. It does not include when visitors or performers supply their own personal protection service, unless the plan has specific provisions for accommodating such personal protection service (e.g., special quarters or security activities such as bomb sweeps).

Does the facility notify or communicate security information to personnel?

"No" means no security information is communicated to company personnel (e.g., only emergency plan information such as evacuation or fire drill information).

Specific security incident information is for an actual security incident (e.g., suspicious people have been observed around the facility back doors, a change in NTAS level, or how to thwart known attempts at hacking the company IT servers).

Recurring security awareness information is communicated regularly to personnel through some means (posters, emails, security announcements).

Security Management Profile	
Are background checks conducted?	☐ No ☐ Yes *If yes,* Background checks are conducted on [check all that apply]: Employees (except security) ☐ All employees (including critical employees, temporary employees) ☐ Not all employees Are recurring background checks conducted? ☐ No ☐ Yes Employee Security Personnel ☐ N/A ☐ No ☐ Yes Are recurring background checks conducted? ☐ No ☐ Yes Contract Security Personnel ☐ N/A ☐ No ☐ Yes Are recurring background checks conducted? ☐ No ☐ Yes Contractors ☐ N/A ☐ No ☐ Yes Are recurring background checks conducted? ☐ No ☐ Yes Vendors ☐ N/A ☐ No ☐ Yes Are recurring background checks conducted? ☐ No ☐ Yes
Background Checks Briefing Notes: _____	

Are background checks conducted?
It is understood that there may be limitations to background checks in some states or for foreign contractors. The intent of the question is to determine if there is a process for background checks. Often background checks are a r easonable action to dissuade insider threats or to ensure effective hiring practices. If foreign contractors do n ot have background checks, but are allowed to be in the facility without restrictions, then do not select Contractors/support functions.

For the types of people that are required to have background checks, check all that apply. If you check All Employees, you do not have to check Critical Employees or Employee security personnel; they are included in all personnel. However, if only the employee security personnel have background checks and no all personnel, just check that. Security personnel, however, may be employees or contractors; therefore, they are listed separately. Since contract security personnel usually have some kind of background checks through their company, it is listed separately from general contractors.

N/A means the people of that particular sub group do not visit or enter the facility. No contractors, or security personnel, or vendors.

Security Management Profile	
Does the facility utilize sensitive internal company information?	☐ No ☐ Yes
	If yes, is sensitive internal company information identified? ☐ No ☐ Yes
	If yes, is sensitive information protected, stored, accessed, transmitted, and destroyed? ☐ No ☐ Yes *If yes: (Check all that apply)* ☐ Secure Storage ☐ Locked file cabinets ☐ Locked room ☐ Limited access (password protected) ☐ Adequately Destroyed (e.g., shredding, burning) ☐ Protective Markings ☐ Secure transmission ☐ Security review of information disseminated to the public (e.g., internet postings)
	If yes, does the facility have security containers? ☐ No ☐ Yes If combinations are used: ☐ Combinations are changed on schedule ☐ Combinations are changed when personnel are terminated or moved ☐ Combinations are recorded and secured ☐ Security containers are located where they can be observed by guards making rounds
Sensitive Information Briefing Notes: _____	
Security Management Profile Overall Comments: _____	

Sensitive information is protected, stored, accessed, transmitted, and destroyed
First ascertain if the company identifies certain corporate information as sensitive (e.g., critical asset maps and security/business continuity planning documents). In order to answer yes the information is protected and to select any of the types of protection, it is understood that such protections are formal plans or policies and appropriate training/implementation has been completed.

Does the facility have security containers?
Security containers are more than a key-lock file cabinet or a locked room indicated in the previous question. A security container would have a special combination or a file cabinet with an outside bar attachment with a special lock. If they have a combination, answer the follow-up questions concerning combinations.

Resilience Management Profile	
Resilience Operations	Is there a manager/department in charge of business continuity? ☐ No ☐ Yes if yes, is this the primary function of that manager/department? ☐ No ☐ Yes
Does the facility participate in any emergency preparedness working groups?	☐ No ☐ Yes *If yes,* ☐ Federal-level emergency preparedness working group ☐ State-level emergency preparedness working group ☐ Local-level emergency preparedness working group ☐ Private Sector /Industry emergency preparedness working group Describe: _____
Does the facility have a written business continuity plan?	☐ No ☐ Yes *If yes,* The plan is developed at the: ☐ Corporate-level ☐ Facility-level Has the plan been approved by senior management? ☐ No ☐ Yes Is the plan required by a Federal, state, or local regulation? ☐ No ☐ Yes

RESILIENCE MANAGEMENT PROFILE

Is there a person and/or a group ensuring collaboration/coordination of resilience related activities (i.e., business continuity, emergency management, security management)?

A business continuity manager creates and executes plans to keep a company functioning after disruptive events such as natural disasters, terrorism, crime and computer and human error. They conduct business impact analysis and risk assessment that includes critical assets, functions (e.g., IT systems), building facilities, personnel and supply chain. They may be called a continuity coordinator or disaster recovery manager, a certified business continuity professional or specialist, project manager, crisis manager, emergency manager, or other title, but, the function is to implement business continuity management within the organization or enterprise of which the facility or asset is a part.

Resilience activities may fall under different functions performed by different people and/or groups in the organization. The intent of this question is to characterize if resilience, in general, is one of the elements considered in the management organization.

Does the facility have a business continuity plan?
Does the facility have a written emergency action/emergency operation plan?

It may be that the facility has an integrated crisis management plan, which includes all emergency response functions. If this is the case, still answer the questions for the appropriate section of that integrated plan. Emergency Action Plan would normally address things like weather, fire related responses such as evacuation or shelter-in-place activities, and bomb threats or checklist type items.

Resilience Management Profile	
Does the facility have a written business continuity plan?	Has the plan been coordinated with stakeholders (e.g., customers or regulatory agencies)? ☐ No ☐ Yes If yes, Is the plan reviewed annually with stakeholders ☐ No ☐ Yes Are key personnel aware of and do they have access to a copy of the plan? ☐ No ☐ Yes Are personnel trained on the plan? ☐ No ☐ Yes If yes, ☐ Key personnel only are trained on the plan [*check all that apply*] ☐ At initial employment ☐ At least once a year. OR ☐ All personnel are trained on the plan [*check all that apply*] ☐ At initial employment ☐ At least once year
	Is the plan exercised at least once a year: ☐ No ☐ Yes If yes, these exercises are: ☐ Tabletop (practical or simulated exercise) ☐ Includes external responders ☐ Functional (walk-through or specialized exercise) ☐ Includes external responders ☐ Full scale (simulated or actual event) ☐ Includes external responders Are exercise results documented, approved and reported to executive management? ☐ No ☐ Yes

BUSINESS CONTINUITY PLAN

The development and implementation of a business continuity plan is vital to the overall resilience of any organization. Business continuity is formally defined as a "comprehensive managed effort to prioritize key business processes, identify [hazards] to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to challenges that surface during and after a crisis" (ASIS 2005). A business continuity plan contributes to reducing organizational consequences and enhancing an organization's ability to continue essential operations after an incident. This document provides an overview regarding the core components of effective business continuity plans and a framework for the development of tailored, organization-specific plans.

The purpose of a business continuity plan (BCP) is to enable an organization to recover or maintain its activities in the event of a disruption to normal business operations (BS25999-1:2006). A BCP plans against any event that could impact critical operations or could have a negative impact on the company and/or facility. For example, NATO planning would be part of business continuity plan.

This process should address large-scale incidents – such as natural disasters or terrorist attacks – as well as smaller disruptions such as supply chain partner problems or the absence of key staffers.

Additional Information:

- British Standards Institute (BSI) 25999 Standard on Business Continuity
- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs
- ANSI/ASIS SPC.1-2009 Standard on Organizational Resilience
- ISO 22301 Societal Security – Business Continuity Management Systems – Requirements 06-15-2012

In this section, we want to capture **procedures necessary for the continuation of facility's functions** (e.g., critical suppliers/materials, key personnel with special skills, alternate site of business, or employee communications for relocation).

If the facility has written documentation of any of the procedure presented under business continuity plan, it should be captured here even if the facility does not have a plan specifically named "Business Continuity Plan".

Note: Cyber service continuity and disaster planning is presented under Dependencies Information Technology.

Does the facility participate in any emergency preparedness working groups?

The intent of this question is to capture if the facility, or one of its representatives, meets on a regular basis with other people to share expertise and prepare to better respond to an emergency.

ISO 22301 and ASIS SPC.1-2009. Under the general heading of warning and communication, does the facility have structured communication with emergency responders. In addition, participation in working groups provides the facility access to other organization's procedures and processes, to better prepare for emergencies. Other groups may include regional resilience programs or groups, regional or even local risk management or business continuity groups or organizations.

Does the facility have a written business continuity plan?

ISO 22301, 8.4.4. Establish documented procedures for responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe.

Best practices based on BS 25999 and ASIS SPC.1-2009 suggest the plan should be supported at the senior management level. If required by some regulation is informational but helps explain why or why not a plan may exist.

This page is intentionally left blank

Are personnel trained on the plan?

The intent of this question is to capture if facility personnel know the plan and its content (procedures), in addition to their role in the case of an incident. ISO 22301 indicates that exercises can validate training provided.

Are exercise results documented, approved and reported to executive management?
Documentation of training and exercises: Part of the process of creating an auditable trail is to document the exercise or training results.

Resilience Management Profile	
Does the facility have a written business continuity plan?	Does the business continuity plan include *(check all that apply)*: ☐ Business continuity plan activation ☐ Immediate (operational) mitigation measures/strategies for responding to the disruption and prevent further loss ☐ Interim (tactical) mitigation measures/strategies for responding to the disruption and prevent further loss ☐ Long-term (strategic) mitigation measures/strategies for responding to the disruption and prevent further loss ☐ Identification of pertinent risks and hazards Does the business continuity plan identify critical processes and as sets necessary for core operations? ☐ No ☐ Yes For these processes and assets, has the facility conducted an impact evaluation that considers the following: ☐ Financial ☐ Customer service ☐ Work backlog ☐ Third party relationships and interdependencies ☐ Regional, national and international considerations (e.g., cascading effects) ☐ Health and safety of persons in the affected area ☐ Regulatory and contractual obligations ☐ Reputation or consumer confidence ☐ Recovery Point Objectives ☐ Recovery time objectives for each key product or service identified

Does the business continuity plan include:
This list of items is based on ISO 22301, ASIS SPC.1-2009, NFPA 1600 and BS 25999 and is part of the Plan, Do Check Act model used in the standards.

Immediate (operational) mitigation measures/strategies for responding to the disruption and prevent further loss, Interim (tactical) mitigation measures/strategies for responding to the disruption and prevent further loss, Long-term (strategic) mitigation measures/strategies for responding to the disruption and prevent further loss. These items are indicators of protection and mitigation but also lead to response and the planning for recovery. Immediate actions may include a graceful shut down of a process, moving items from rising water, or conducting data backups. Interim actions may include moving certain items, people, or processes to another facility, calling in additional help from or assistance teams locally or from within the region, or coordinating with responders to shore up a dike or flood wall. Long term activities may include developing plans and obtaining funding for a permanent fix to a flood problem, establishing a permanent backup facility, or construction to improve the structural soundness of a given asset or facility.

For these processes and assets, has the facility conducted an impact evaluation that considers the following:
Based on the identified hazards, the team should conduct a business impact analysis to evaluate the potential damage or loss to the organization resulting from a disruption (ASIS 2009; BCI 2010; NFPA 2010). To complete this phase, the planning team should (1) define the potential impacts of each of the hazards identified as potentially affecting the critical functions of the organization; and (2) determine the minimum resources needed to continue operations at the lowest acceptable level for a predicted timeframe. The answers to these questions will impact how potential risk reduction measures are prioritized in the plan. Although this step can be complex, conducting a thorough business impact analysis is vital to an effective business continuity strategy. It will help define the recovery priority and the Recovery Time Objective.

Work backlog
An accumulation of uncompleted work, unsold stock, etc. to be dealt with when business is resumed.

Third-party relationships
Commonly referred to as “outsourcing” it can include contract support for IT, auditing, insurance, etc.

Recovery Point Objectives
Recovery Point Objective (RPO) is the point at which processes or activities must be restored in order to resume operations. For example, if left unheated a chemical will solidify and ruin the storage tanks or so much data is lost for a cyber system that there is no recovery.

Recovery time objectives for each key product or service identified
Recovery Time Objective (RTO): Period of time following an incident within which the product must be received (e.g., raw materials) or the service restored (e.g., internet) or the resource recovered (e.g., the electric comes back on) before the RPO is reached.

The plan defines the recovery time objectives for each key product and service that is essential to operations. For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable (i.e., the RPO) .For example, for the healthcare sector, continuation of patient care is a recovery point objective and 30 minutes is the recovery time objective before patients must be moved.

Resilience Management Profile	
Does the facility have a written business continuity plan?	Does the business continuity plan have procedures for *(check all that apply)*: ☐ Maximum Acceptable Outage (MAO) ☐ Trigger points that identify activation of plans, notification, or other actions ☐ An up-to-date point of contact roster for: ☐ Key personnel responsible for continuity activities (e.g., organizational resilience or crisis management teams) ☐ Essential infrastructure contacts (e.g., utilities, suppliers, providers) ☐ Alert and notification to employees ☐ Identification of personnel with special skills, education or training ☐ Identification of alternates ☐ Location and relocation procedures ☐ Safe close-down procedures ☐ Adequate security / property protection if closed or relocated ☐ Communication and coordination for continuity activities with other stakeholders (e.g., customers, regulatory agencies, Local Law Enforcement or response agencies) ☐ Notification to suppliers/utility providers ☐ Alternative work arrangements (e.g., telecommuting or assignment to other corporate locations)/ Virtual office options ☐ Designated crisis management center, emergency operations center or an incident management and command center (IMCC) ☐ Identification of key emergency personnel by position ☐ Identification of alternates ☐ IT recovery ☐ Decision process for activation and relocation ☐ Exercising of the plan ☐ Alternate sources for customers (e.g., other corporate facilities or contracts with competitors) ☐ Plan maintenance (e.g., review and revision) ☐ Pandemic response ☐ Human resource procedures (e.g., employee counseling, financial support, payroll) ☐ Reconstitution of normal operations ☐ Insurance program for acceptance/retention and transfer of risk ☐ Devolution (e.g., closing the original facility) ☐ None of the above
Business Continuity Plan Briefing Notes: _____	
Overall Business Continuity Plan Comments: _____	

Does the business continuity plan have procedures for (check all that apply):

Maximum Acceptable Outage (MAO)
Maximum period of time that the critical business processes can operate before the loss of those critical resources affect their operations. This is the time it would take for adverse impacts which might arise as result of not providing a product/service or performing an activity to become acceptable.

Trigger points that identify activation of plans, notification, or other actions
Based on the facility characteristics and missions, and the Maximum Acceptable Outage (MAO), the trigger points are the criteria that define when specific business continuity actions and procedures should be implemented for reducing the consequences of an event.

Alert and notification to employees
This could include call down lists, call-in numbers, emails, or electronic bulletin boards; anything that would allow the employee to find out whether they should come in to work, stay home, or report to a different location.

Identification of personnel with special skills, education or training
These would be people that would be essential to continuing the facility's operations such as IT support, repair personnel, or administration support.

Decision process for activation and relocation
This would be a written decision process for determining when to implement the plan and when to move to each phase of the plan, including who makes this decision and what factors must be present to make such a decision.

Exercising the plan
This section outlines how essential equipment or a process is tested, how employees and key personnel are trained and or evaluated on the plan and the regimen for exercising the plan.

Alternate sources for customers (e.g., other corporate facilities or contracts with competitors)
Some facilities may have backup plans for providing customers with goods or services through other contracts (e.g., hospitals may have a plan for transferring patients to other nearby facilities in the event of a business interruption or a chlorine repackager may have a standing contract with another sister company or even a competitor to provide chlorine to an essential customer.

Pandemic response
These provisions may include several strategies discussed above, but specially established for a disease scenario. For instance, during a pandemic situation, companies may have provisions for alternative work arrangements or for identifying alternates for essential positions.

Resilience Management Profile	
Is there an alternate site for continuity of business?	☐ No ☐ Yes If yes, for any alternate site is there: ☐ Full capability ☐ Sufficient distance between the alternative facility and the original facility (e.g., not in the same flood zone or explosion zone) ☐ Capability to perform essential functions quickly and for an extended period ☐ Reliable logistical support, services and infrastructure systems (e.g., utilities and backup generator) ☐ Adequate security systems ☐ Communication support ☐ Activation or use during exercises ☐ Transportation support (e.g., sufficient parking) ☐ Sufficient computer equipment and software ☐ Access to vital files, records and databases ☐ Sufficient space and equipment ☐ Alternate modes of obtaining supplies (e.g., rerouting to alternate site or finding other local suppliers – supplier contract issues) ☐ Consideration for health, safety and emotional well-being of personnel ☐ Limited or no dependencies in common with the primary site ☐ None of the above
Alternate Site Briefing Notes: _____	
Overall Alternate Site Comments: _____	

ALTERNATE SITE

Is there an alternate site for continuity of business?
Key features of an alternate site include its characterization and the percent of the normal level of the main facility's production it can handle.

This would be the core operations are moved to an alternative site. For instance, the data control center can operate from another data control center in another city; that is an alternative site. If a team can play in another stadium (e.g., when the Bears played at the University of Illinois while their stadium was being modified), that is another example of an alternate site. However, the fact that people can shop at an alternate mall is not an alternate site for the facility being assessed. The fact that there are other hotels in the area is not an alternate site. Also, if the only thing that has an alternate site is the data center and all other core functions cease, then perhaps it is not an alternate site. If the core mission is carried out remotely from employee's homes, for instance, that is not an alternate site. Facilities like manufacturing, hospitals, hotels, malls, bridges, tunnels, stadiums, arenas, racetracks, casinos, most general office buildings and similar facilities rarely have an alternate site. Data centers, government agencies / functions, banking and communication facilities often have an alternate. For instance, redundant data center where data is backed up but operating terminals would have to be programmed/updated (e.g., cold site) or operational control center at corporate sister plant where operators can instantly log in as if they were located at the original location (e.g., hot site).

For any alternate site is there:
Full capability
The alternative facility can carry on all essential business functions. There may be some loss of non-essential functions and still be considered full capability. For instance, a relocated data center may be able to process all business essential IT functions, but cannot directly backup to the central servers or a customer call center may be able to take care of everything, including dispatch, except setting up new web-based accounts.

Sufficient distance between the alternative facility and the original facility
Sufficient distance can be defined as the alternate site does not rely on the same services as the original facility (transportation, water, power) and is not in the same zone of hazard (e.g., two blocks from the original site but in the same flood zone).

Capability to perform essential functions quickly and for an extended period
This is similar to full capability, but includes the ability to start up immediately, without installation of new equipment or reloading underlying IT platforms/programs/applications (uploading updated data may be necessary).

Communication support
This would include adequate telephone service, radio capability or fiber connections at the alternate facility as necessary to conduct business.

Transportation support
This refers to the ability of employees to drive and park, commute via public transportation, or company-provided transfer from the original location.

Access to vital files, records and databases
This access can be via backup tapes/discs or an alternative server system. It can also be paper copies that allow the continuity of business in a reasonable fashion. For instance, loss of a customer service center may require the company to resort to paper dispatch forms that are faxed to the repair teams.

Alternate modes of obtaining supplies (e.g., rerouting to alternate site or finding other local suppliers – supplier contract issues)
Existing contracts or supply modes may not be available in the new location if it is far from the original facility, so new contracts or methods of obtaining regular supplies such as office supplies, repair parts, or essential services (e.g., copier maintenance support) may be needed for the alternate location.

Consideration for health, safety and emotional well-being of personnel
This may include counselors, employee assistance programs for finding temporary housing, transportation, and family accommodation.

This page is intentionally left blank

Limited or no dependencies in common with the primary site

Related to sufficient distance, does the alternate site depend on the same resources such as substations, water and wastewater utilities (or utility zones), communication offices/towers, etc.

Resilience Management Profile	
Resilience Management	Is there a manager/department in charge of emergency management? ☐ No ☐ Yes if yes, is this the primary function of that manager/department? ☐ No ☐ Yes
Does the facility have a written Emergency Operation/ Emergency Action Plan?	☐ No ☐ Yes *If yes,* The plan is developed for: ☐ Corporate-level ☐ Facility-level Has the plan been approved by senior management? ☐ No ☐ Yes Is the plan required by a Federal, state, or local regulation? ☐ No ☐ Yes Has the plan been coordinated with emergency responders? ☐ No ☐ Yes If yes, is it reviewed annually with emergency responders? ☐ No ☐ Yes Are key personnel aware of and do they have access to a copy of the plan? ☐ No ☐ Yes

EMERGENCY OPERATION / EMERGENCY ACTION PLAN

An emergency operation / emergency action plan (also called Incident Action Plan) reflects the overall incident strategy, tactics, risk management, and member safety that are developed (NFPA1600).

In this section, we want to capture **procedures for disaster/incident management** (e.g., HAZMAT cleanup, evacuation, shelter-in-place or medical emergencies).

If the facility has written documentation of any of the procedure presented under Emergency operation / emergency action plan, it should be captured here even if the facility does not have a plan specifically named “Emergency Operation Plan or Emergency Action Plan”.

Has the plan been approved by senior management?
The intent of this question is to capture if the plan is supported by the management that is able to embed the implementation of business continuity in the organization’s culture. “Senior management groups” implies all management that relates to business continuity (e.g., building management, engineering management)

Resilience Management Profile	
Does the facility have a written Emergency Operation/ Emergency Action Plan?	Are personnel trained on the plan? ☐ No ☐ Yes If yes, ☐ Key personnel only are trained on the plan [*check all that apply*] ☐ At initial employmen ☐ At least once a year. OR ☐ All personnel are trained on the plan [*check all that apply*] ☐ At initial employment ☐ At least once year Is the plan exercised at least once a year? ☐ No ☐ Yes If yes, these exercises are: ☐ Drill (e.g., fire drill) ☐ Includes external responders ☐ Tabletop (practical or simulated exercise) ☐ Includes external responders ☐ Functional (walk-through or specialized exercise) ☐ Includes external responders ☐ Full scale (simulated or actual event) ☐ Includes external responders Are exercise results documented, approved and reported to executive management? ☐ No ☐ Yes
	Does the emergency action plan have procedures for *(check all that apply)*: ☐ Change in the hazard environment ☐ Increased communications and notification ☐ Establish real-time communication between emergency management and decision-level executives ☐ Additional infrastructure upgrades/redundancy ☐ Enhanced incident response (e.g., initiated MOU with Local Law Enforcement or Fire Department) ☐ Initiate Planning and preparedness ☐ Pre-assign emergency response Personnel (on-call) ☐ Assign emergency response personnel to pre-planned positions/roles ☐ Prepare to execute contingency procedures ☐ Execute contingency procedures ☐ HAZMAT spills/releases ☐ Appropriate natural hazards for the region

Initiate Planning and preparedness can be any or all of the following:

Prepare to execute contingency procedures.

An example is when a plan has phases, such as port hurricane condition declarations by the USCG trigger different mitigation measures: Whiskey & X-Ray a m aritime transportation facility would remove vessels from its docks out to open sea, at Yankee, the facility would move heavier equipment around tanks and lighter containers in the staging area and shutter their office windows, at Zulu, they would evacuate the premises except for selected response crews.

Resilience Management Profile	
	☐ Terrorist events ☐ Active shooter ☐ Internal disturbances (e.g., workplace violence) ☐ Hostage situations ☐ Shelter-in-place ☐ Medical emergencies/Medical surge ☐ Fire ☐ Bomb threat ☐ Chemical/Biological/Radiological attack ☐ Incident in nearby facilities that would impact facility's operations ☐ Cyber attack (may be a separate plan) ☐ Extended utility loss (e.g., blackout) ☐ Civil unrest/Riot ☐ Strike/Lockout ☐ Explosion ☐ An up-to-date point of contact roster for: ☐ Key personnel responsible for emergency activities (e.g., crisis management teams) ☐ First responders ☐ Essential infrastructure contacts (e.g., utilities, suppliers, providers) ☐ Emergency communications to employees and stakeholders (e.g., telecommunications service priority (TSP), Government Emergency Telecommunications Service (GETS) and wireless priority service (WPS)) ☐ An emergency coordinator with specific duties assigned ☐ Route(s) for evacuation ☐ Exercising the plan ☐ Plan maintenance (e.g., review and revision) ☐ None of the above
Emergency Operation / Emergency Action Plan Briefing Notes: _____	
Overall Emergency Operation / Emergency Action Plan Comments: _____	

Incident in nearby facilities that would impact facility's operations
The plan should include any mitigation measures for incidents at neighboring facilities if it can impact the facility or its personnel. An example would be to have shelter-in-place kits with plastic and tape when the facility is next to a chemical plant that has a public warning siren to warn of the release of a dangerous air-borne chemical (e.g., hydrofluoric acid).

Routes for Evacuation
This could be building diagrams with evacuation routes or hurricane evacuation route directions.

Exercising the plan
This section outlines how essential equipment or a process is tested, how employees and key personnel are trained and or evaluated on the plan and the regimen for exercising the plan.

Resilience Management Profile	
Does the Facility have immediate onsite response capability for?	☐ Toxic industrial chemical/HAZMAT release ☐ able to handle incident without the aid of external responders ☐ Fire fighting ☐ able to handle incident without the aid of external responders ☐ Bomb Threat (e.g., render safe) ☐ able to handle incident without the aid of external responders ☐ Armed response ☐ able to handle incident without the aid of external responders ☐ Law enforcement (e.g., mass transit police) ☐ able to handle incident without the aid of external responders ☐ Medical Emergency ☐ able to handle incident without the aid of external responders ☐ None of the above
Onsite Capabilities Briefing Notes: _____	

Does the Facility have immediate onsite response capability for?
This initial question is looking for the basics and includes automated external defibrillators (AED), fire extinguishers, people trained in cardiopulmonary resuscitation (CPR), etc.

Able to handle an incident without the aid of external responders?

Intent is to identify whether the facility can respond to a significant incident with its own onsite response capability. For example, if a facility has firefighting capability, the answer is YES if the facility has a trained, equipped firefighting team for managing fires at the facility and NO if the only response capability is the presence of fire extinguishers and awareness training. The answer will be YES only if the facility does not need immediate external support. It is assumed that all facilities would contact and or notify the appropriate agency (or 911) if a significant event occurred.

Resilience Management Profile	
Does the facility exchange information with a local or state Emergency Operation Center?	☐ No ☐ Yes
Does the facility have an Incident Management and Command Center (IMCC)?	☐ No ☐ Yes *If yes,* Where is the primary IMCC located? ☐ Onsite ☐ Offsite Has the primary IMCC been activated in the previous year (whether through an exercise or event)? ☐ No ☐ Yes Following the activation was an after action report completed? ☐ No ☐ Yes Can the IMCC operate independently of all outside utilities for at least 72 hours? ☐ No ☐ Yes Does the IMCC contain the following elements? ☐ Sleeping Quarters ☐ Dining/Food Preparation Space ☐ Briefing Areas ☐ Portable Restrooms (Backup) ☐ Communications Area ☐ Adequate Parking ☐ Proper Equipment and Backup

INCIDENT MANAGEMENT AND COMMAND CENTER (IMCC)

Does the facility have an incident management and command center?

An Incident Management and Command Center (IMCC) is defined as any room or area specifically designated by the facility as the central location from which the facility would manage emergency operations. It is the place where decision makers and key facility emergency personnel or business continuity personnel can gather during an emergency. It could be called something other than Incident Management and Command Center, e.g., Security Control Center, Operations Control Center, or even Break room.

Has the primary IMCC been activated in the previous year (whether through an exercise or event)?

Activation would include opening the facility, operating any emergency equipment or communications, gathering key personnel, etc.

Can the IMCC operate independently of all outside utilities for at least 72 hours?

The intent of this question is to capture if the IMCC has everything needed (equipment, medical supplies, food, water, etc.) to fulfill its mission for at least 72 hours.

Does the IMCC contain the following elements?

For the list of items (Sleeping Quarters, Dining/Food preparation Space Briefing Areas, Portable Restrooms (Backup), Communications Area, Adequate Parking, Proper Equipment and Backup), there are no specific values assigned or determined. While the list is more of a reminder checklist of items to include, if provided the opportunity to view the area or discuss this area consider the type of facility, the area being used, the number of people the company has indicated would occupy the area and the communication needs. If this is a refinery, manufacturing facility or some other very large organization and they use massive technology and communications and indicate they need 20 people to run the IMCC, but the room is small office with a single phone, it may not meet the facility needs.

Resilience Management Profile	
Does the facility have an Incident Management and Command Center (IMCC)?	Is there a backup IMCC? ☐ No ☐ Yes Is the backup IMCC site geographically separated from the primary IMCC site? ☐ No ☐ Yes Can the backup IMCC operate independently of all outside utilities for at least 72 hours? ☐ No ☐ Yes
Incident Management and Command Center Characteristics Briefing Notes: _____	
Overall Resilience Management Profile Comments: _____	

Is the backup IMCC site geographically separated from the primary IMCC site?
Geographically separated so as to not be in the same "zone of hazard". If they are in the same building, the loss of the building would impact both IMCCs.

Can the backup IMCC operate independently of all outside utilities for at least 72 hours?
The intent of this question is to capture if the backup IMCC has everything needed (equipment, medical supplies, food, water, etc.) to fulfill its mission for at least 72 hours.

Security Force Profile	
Does the facility have a security force?	☐ No ☐ Yes If yes, Onsite security force ☐ No ☐ Yes Offsite security force **only** (no onsite force) ☐ No ☐ Yes
	If yes to either onsite or offsite security force: Is there a Surge Capacity Plan? ☐ No ☐ Yes *If yes,* Surge Capacity Plan has the following Personnel: ☐ None ☐ Law Enforcement [MOA/Contract/Off-duty] ☐ Contracted Security ☐ Other organization/corporate
	Arrest Authority ☐ No ☐ Yes Detain Authority ☐ No ☐ Yes

SECURITY FORCE PROFILE

Does the facility have a security force?
A security force is a special group of employees or contractors with security duties. Security force does not include general employees who are trained in security awareness to observe and report in addition to their regular duties. Although there are many facilities that will indicate that a receptionist, ticket taker, usher, or janitor are the security force, in the IST /SAV definition those personnel are not considered security force personnel. This methodology defines security force as individuals with unique and sole duties to provide security.

Whether a facility has a security force may depend on the definition of the "facility." For instance, a facility may be a banking facility occupying several floors in an urban high-rise. The "facility" does not have its own security force for just those floors; however, the building provides security guards that control access to the upper floors of the building, including the facility. In this case, the facility may have a security force protecting their perimeter through a contractual relationship (its lease) with the building owner. It is important to determine if these security guards actually provide access control or if they are simply lobby attendants that provide direction.

Onsite security force is one that is stationed at the facility. This requires an onsite presence, assigned to and responsible for a given facility location. Examples include a security guard at a chemical plant, guards in an office building lobby, the security guards at a museum.

An offsite security force is one that may patrol the facility occasionally, but are not stationed there. For example, railroad and transit police forces may cover a large area with a number of facilities and will only visit the facility periodically (e.g., once per shift, daily, or weekly). This also includes situations where a main office may be at a given facility, but the security force only "checks in" or conducts role at that location, and the rest of their duties are conducted at other locations.

Surge Capacity Plan
This is a plan to provide additional security force during a special circumstance or elevated threat. An example may be a chemical plant or refinery that has a surge plan to bring in 10 off duty police officers in times of increased threat. Or a facility has a plan to bring in a contract security force during a natural disaster when the normal employees cannot get to work or have been provided time to recover. Identify the types of personnel used to staff this plan. For most facilities, continue to answer the security force questions for the usual onsite or offsite security force.

Public venues such as such as stadiums, arenas, and racetracks should be assessed or viewed as if it is "event day" or "game day". Typically this type of facility has a small security force or guard force day to day, but a large contingent of security during the specific event. This surge of security personnel may vary in number and type depending on the specific event occurring. A concert may have more or less security than a NFL football game at the same venue. Ticket takers, ushers, volunteers and others that have observe and report responsibility in addition to other duties during the event are not considered security force personnel. When answering the remaining security force questions for a public venue select the responses based on the most capable force indicated by the selections in the surge capacity plan. This will normally be local law enforcement as most capable, followed by contract and then other organizations / corporate. As an example, an NFL stadium day to day has 5 security guards that secure the facility from 7 AM to 6 PM and then they lock the doors and leave. However leading up to and during the event 100 law enforcement agents from 6 agencies, 120 contract guards from 3 different companies and 20 NFL security specialists are added to the security force for the duration of the game and a few hours after. Base your answers on the 100 law enforcement agents.

This page is intentionally left blank

Law Enforcement [MOA/Contract/Off-duty]
A security force could include off-duty police officers hired by the facility to augment their own contract or employee guard force. However, the fact that there is a police station across the street, a city police substation within a mall, or even police permanently stationed by the City in a hospital emergency room due to crime issues, would not be considered a facility security force. Those police are not in control of the facility and have no contractual or other responsibility to defend the facility other than their sworn duties.

Contracted Security
If this is not checked, it is assumed the surge security force is proprietary (e.g., made up of company employees)

Other organization/corporate
Sometimes, particularly for special events, a facility may establish agreements with a volunteer team of off duty officers or non-security personnel. Sometimes a facility may establish agreements with a nearby or adjacent facility. The other area this may cover is if corporate headquarters for the facility sends in an additional security force from elsewhere in the country.

Arrest Authority
Authority granted by federal or state statute or regulation to sworn officers to execute a legal arrest. Usually, security officers do not have arrest authority unless they are sworn officers. It may be that off-duty police officers retain their arrest authority even working as a security guard. Otherwise, it is simple common law citizen's arrest and not arrest authority.

Detain Authority
A Detention is a non-consensual temporary denial of liberty. In order to detain an individual, a police officer must have "reasonable suspicion" that:

- They are about to commit a crime
- They are in the act of committing a crime, or
- They have committed a crime

Security Force Profile	
Security Force Staffing	
Security staffing at different types of posts (select types of posts covered by security staff at the facility/SAA)	
☐ Static Posts	**Static Post Coverage** What percentage of SAAs are covered by security force personnel? ☐ 1-25% ☐ 26-50% ☐ 51-75% ☐ 76-99% ☐ 100 % Check the least number of hours any static post is covered by a security personnel: ☐ 8 hours or less ☐ 8-12 hours ☐ 12-18 hours ☐ 18-24 hours
☐ Roving Patrols (e.g., Mobile Posts) Select all that apply ☐ Predetermined sequence ☐ Random	**SAA Coverage** What percentage of SAAs are covered by roving patrols? ☐ 1-25% ☐ 26-50% ☐ 51-75% ☐ 76-99% ☐ 100 % Of those SAAs covered by roving patrols, provide the one with the least frequent patrol: ☐ At least once every hour ☐ Once every 1-8 hours ☐ Once every 8-24 hours ☐ Less frequently than every 24 hours
Security Force Staffing Briefing Notes: _____	

Security staffing at different types of posts (select types of posts covered by security staff at the facility/SAA)

Security Force Staffing captures whether the facility has sufficient security force to cover all of the facility or SAA's either through static posts, or roving patrols. Staff should be answered for normal facility operations. The only exception would be for public venues when the threat is against the patrons attending an event and, therefore, the IST is being completed for the event day.
For public venues (e.g., stadiums, arenas and racetracks, convention centers), security could be provided by law enforcement, contract or corporate personnel. Volunteers, ticket takers and ushers are not considered security force in this methodology.

Static Posts
Static posts are positions manned by stationary personnel for entry control, monitoring and/or protection. Static posts may be located at a significant area or asset, but also could be at other areas where the facility has determined an attendant is necessary to monitor the security of the area, such as a loading dock, casino floor, hospital waiting room or lobby. This also includes personnel stationed at an entry/access control point, such as a gate or door, to control entry. Static posts also include personnel designated to monitor facility command and control centers. It does not however include positions that monitor CCTV or an IDS. That is captured in the respective sections.

Roving Patrols
Security personnel that move around the facility or cover a large area to check that security has not been breached or to watch for potential indicators of trouble. In some cases a facility may have both, especially if it is a public venue.

For each type of post:
Static Posts
First determine the number of static posts that have been established by the facility. Then determine who is stationed at each of these static posts. For instance, there may be two entry control points to the facility (e.g., a front door and a back door) and one static post for monitoring the cameras in the control center, however, the entry control points are staffed by non-security personnel, such as a receptionist and only the control center is staffed by security force personnel. In this case, only one-third of the three static posts are staffed by the security force (i.e., 33.3%) and one would select the 26-50% box. If there are no security personnel stationed at static posts established at the facility, do not check the box for static post.
If there are three static posts, as described in the example above, and none are staffed by security personnel, such that the percentage of coverage is 0, **then do not check the box for static posts** since there is no security force coverage for static posts and do not complete any of the questions about coverage or hours.

For a public venue it may be determined that there are 300 static posts. Some could be at entry points, some could be on the playing field, and some may be at strategic locations near SAA's. If 200 of these 300 static posts are staffed by ushers or other with observe and report responsibility, they are not security force, thus only one third (33%) are covered by a security force.

Determine the number of hours these static posts are covered. If the entry control points are staffed only during business hours (e.g., a 12-hour shift) but the control room monitoring post, which is the only static post monitored by security personnel, is staffed 24/7. Therefore, since this section is addressing security personnel staffing the least number of hours that any static post is staffed by security personnel is 24/7, select the box for 18-24 hours.

For a public venue, answer the percentage coverage and number of hours of coverage for the most capable surge security force present on event day. For instance, if the public venue has local law enforcement as some part of its surge capacity plan and there are local law enforcement personnel at each static post, then mark 100% of static posts are covered. However, if only non-security personnel, with just “observe and report” authority, occupy the 16 public entry/access control points (e.g., ticket takers), and there are six other static posts staffed by the local law enforcement personnel that make up the surge security force (e.g., the locker room door and five podiums that monitor the public areas), then select the box for 26-50% (22 static posts – 16+6 – divided by 6 security personnel = 27.3%).

Security Force Profile	
Specify the equipment available to the security force	Uniformed ☐ No ☐ Yes Armed (i.e., gun) ☐ No ☐ Yes Less than Lethal Weapons ☐ No ☐ Yes *If yes, complete the following* ☐ Taser ☐ Chemical Repellant ☐ Collapsible Baton/Baton ☐ Stun Gun Restraints ☐ No ☐ Yes Body Armor ☐ No ☐ Yes Canine Patrols ☐ No ☐ Yes Communications: ☐ No ☐ Yes *If yes, complete the following* ☐ Radio ☐ Cell Phone with Walkie-Talkie Capability ☐ Duress Alarms / “Panic” Buttons: Portable ☐ Cell Phone ☐ Duress Alarms / “Panic” Buttons: Fixed
Security Force Equipment Briefing Notes: _____	

This page is intentionally left blank

Security Force Profile	
Does security force receive training?	☐ No ☐ Yes, *if yes continue* Training Programs: ☐ Federal/State recognized certificatio ☐ Formal ☐ In-house/Informal ☐ Video ☐ Web-based ☐ OJT (on-the-job training) ☐ None of the above Continuation/In-service training: ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Semi-Annually ☐ Annually ☐ None
If yes, security force receives training in the following topics:	
Emergency Response ☐ Bomb Threat ☐ Break-in ☐ Hostage/Barricade ☐ Fire ☐ Chemical HAZMAT release ☐ Natural Disaster ☐ CPR/First aid ☐ Active shooter ☐ All of the above ☐ None of the above	**Standard Operating Procedures** ☐ Facility-specific SOPS ☐ Communications ☐ ICS/NIMS ☐ Public Relations ☐ Legal Implications ☐ NTAS Increase ☐ Threat Awareness ☐ All of the above ☐ None of the above
Weapons and self defense ☐ Weapons ☐ Less Than Lethal Response ☐ Force Continuum ☐ Self Defense ☐ Use of restraints ☐ All of the above ☐ None of the above	**Screening and Access** ☐ Screening ☐ Search Procedures ☐ IDS ☐ IED recognition ☐ Surveillance Detection ☐ All of the above ☐ None of the above
Overall Security Force Training Briefing Notes: _____	
Do comprehensive post orders exist?	☐ No ☐ Yes
Is there a dedicated command and control or operation center for guard force?	☐ No ☐ Yes If yes, specify location:
Overall Security Force Comments: _____	

Training Programs:

Formal
Formal training is defined as professional, contract, classroom training.

Continuation/in-service training:
Mark the most frequent training, even though different types of training may have different time schedules.

Security training topics
This section is broken into groups of like type training. You can select individual training items, or select the entire grouping by selecting “All of the Above” in one of the groupings.

Comprehensive post orders exist:
Post orders describe the duties to be performed by the guard assigned to a particular post (e.g., the guard at the front desk will check badges, conduct searches). Some may call them Standard Operating Procedures for the guard.

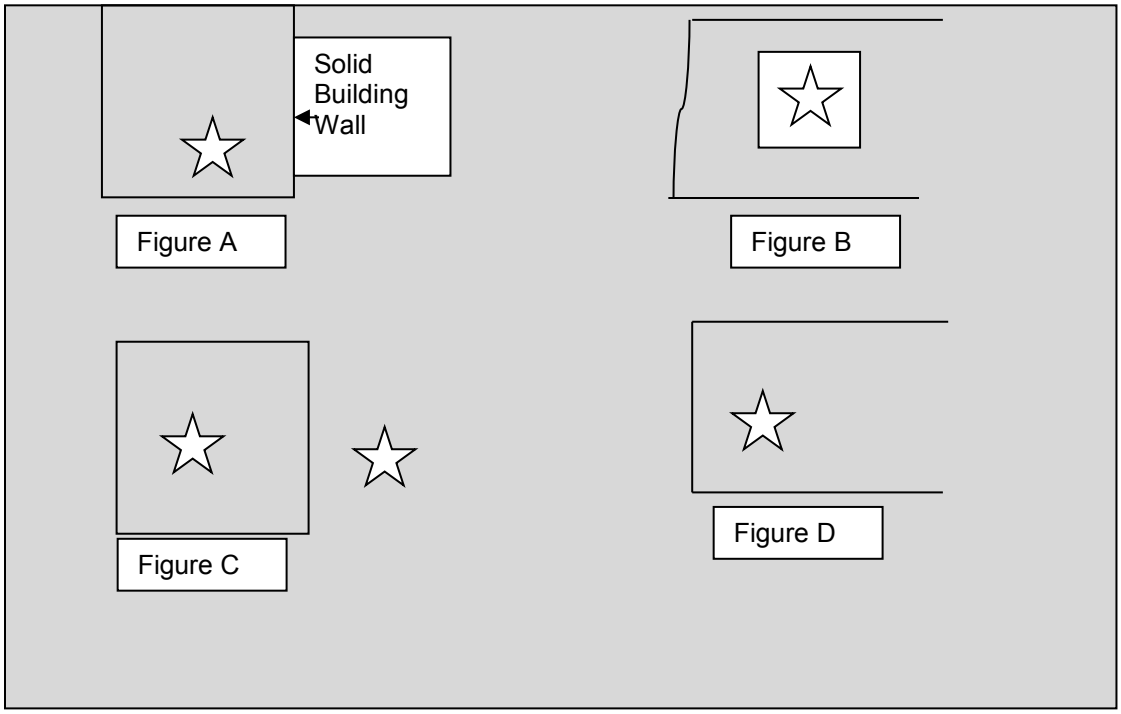
<table>
<tr><th colspan="4">Perimeter Security</th></tr>
<tr><td>Does the facility/SAA(s) have fencing?</td><td colspan="3">☐ No
☐ Yes
If yes, score the rest of section for the weakest section of fence.</td></tr>
<tr><td>Fraction Enclosed</td><td colspan="3">☐ 100% of the facility enclosed AND 100% SAA(s) are enclosed
☐ Less than 100% of the facility enclosed, BUT 100% SAA(s) are enclosed
☐ 100% of the facility enclosed, BUT less than 100% SAA(s) are enclosed
☐ Less than 100% of the facility enclosed AND less than 100% SAA(s) are enclosed</td></tr>
<tr><td>Fence Characterization
(Check all that apply)
(Weakest portion of fence, if type varies)</td><td><u>Type</u>
☐ Chain link
☐ Anti-Climb Aluminum or steel
☐ Standard Aluminum or steel

☐ Other – not chain link
☐ Concrete
☐ Brick and Mortar
☐ Steel
☐ Wrought Iron
☐ Wood
☐ Plastic</td><td><u>Height</u>
☐ Less than or equal to 5 ft.
☐ 5+ ft. – 6 ft.
☐ 6+ ft. – 7 ft.
☐ 7+ ft. – 15 ft.
☐ Greater than 15 ft.

Base of fence
☐ Anchored
☐ Not anchored
☐ N/A (e.g., concrete or brick/mortar wall)</td><td><u>Characteristics</u>
Outriggers (e.g., barbed wire or razor wire)
☐ 45 degrees
☐ “Y” style
☐ Straight up
☐ None

Enhancements
☐ K-rated for vehicle penetration
☐ Second Fence
☐ Electric Fence
☐ Aircraft Cable/Vehicle restraint cable with reinforced anchor points
☐ Coiled razor wire
☐ Coiled barbed wire
☐ Spikes
☐ Privacy screening
☐ None</td></tr>
<tr><td colspan="4">Perimeter Security – Fence Briefing Notes: _____</td></tr>
</table>

PERIMETER SECURITY



Does the facility have fencing?

- ☐ 100% of the facility enclosed AND 100% SAA(s) are enclosed (Figure A)
- ☐ Less than 100% of the facility enclosed, BUT 100% SAA(s) are enclosed (Figure B)
- ☐ 100% of the facility enclosed, BUT less than 100% SAA(s) are enclosed (Figure C)
- ☐ Less than 100% of the facility enclosed AND less than 100% SAA(s) are enclosed (Figure D)

A fence could be a wall or any structure or natural barrier that would prevent entry (e.g., cliff or solid building). Here critical assets are defined as the significant areas or assets (SAAs) (represented by a star below). On rare occasions an SAA can be outside the facility perimeter. For example, a substation that is on facility property, but outside the defined perimeter.

Perimeter Security			
Fence Characterization *(Check all that apply)* *(Weakest portion of fence, if type varies)*	**Type** ☐ Chain link ☐ Anti-Climb Aluminum or steel ☐ Standard Aluminum or steel ☐ Other – not chain link ☐ Concrete ☐ Brick and Mortar ☐ Steel ☐ Wrought Iron ☐ Wood ☐ Plastic	**Height** ☐ Less than or equal to 5 ft. ☐ 5+ ft. – 6 ft. ☐ 6+ ft. – 7 ft. ☐ 7+ ft. – 15 ft. ☐ Greater than 15 ft. **Base of fence** ☐ Anchored ☐ Not anchored ☐ N/A (e.g., concrete or brick/mortar wall)	**Characteristics** Outriggers (e.g., barbed wire or razor wire) ☐ 45 degrees ☐ "Y" style ☐ Straight up ☐ None **Enhancements** ☐ K-rated for vehicle penetration ☐ Second Fence ☐ Electric Fence ☐ Aircraft Cable/Vehicle restraint cable with reinforced anchor points ☐ Coiled razor wire ☐ Coiled barbed wire ☐ Spikes ☐ Privacy screening ☐ None
Perimeter Security – Fence Briefing Notes: _____			

Fence Characterization
The focus should be on the weakest area of the fence **that protects the facility or SAA or entry to pertinent parts of the facility**. For example, the facility may have 8-foot chain link fence with razor wire topper on 99% of the perimeter. However, in one small section the fence is broken or overrun by trees or shrubs and is only 2 feet tall. In this example, although the vast majority of the fence is excellent, the section that is broken creates vulnerability and therefore is the section of fence on which the questions should focus and will be used for scoring purposes. However, consider the location of all SAAs and whether the particular vulnerability in the fence creates a problem. If someone coming through that weak section of fence would be immediately detected, stopped, caught in a mantrap or otherwise prevented from accessing a SAA, then look for another weak section of fence.

It would be unusual for a bridge or tunnel to be 100% fenced. For example, The Golden Gate Bridge may have fence along the side of the roadway for the entire length of the bridge on both sides of the road and other areas such as anchorages and pilings may have fence. The roadway itself is not fenced thus it cannot be 100% fenced. It would also be unusual for a railroad, rail yard, bus route or pipeline to have 100% fencing. If the facility is within a larger complex that is 100% fenced, then the facility has 100% fence coverage. If a facility has a significant asset or area outside of the perimeter fence of the facility, estimate the percentage of that SAA is fenced.

Type:
Anti-Climb Aluminum or steel
Anti-climb includes mesh chain link or any type of aluminum or steel fence that has a very small opening that makes it more difficult to climb or cut. Often this fence has openings in the mesh of 1 inch or less as compared to standard chain link that normally has openings of about 2 inches.

Base of fence: Anchoring is not that just that the fence posts are anchored in the ground, but that there is some additional fixture that prevents crawling under the fence. This can be anchoring the bottom of the fence into concrete, placing anchoring spikes that penetrate the ground at reasonable intervals to prevent the fence from being accessed.

Characteristics:
Outriggers (e.g., barbed wire or razor wire)
It is assumed that the outriggers are equipped with a connecting wire such as barbed wire or razor wire. If they are not, they are not outriggers, but simply extra extensions on the end of the fence posts.

Enhancements:
K-rated for vehicle penetration
To select this option, the fence must have a verified DOS K-rating (4, 8, or 12).

Second Fence
This means that in addition to the fence being described, there is another fence inside that fence protecting the facility or SAA. Think of a prison with a fence, a no-man zone and another fence.

Coiled razor wire or coiled barbed wire
This can be additional razor or barbed wire coiled at the top of the fence within the regular outrigger or coiled at the bottom of the fence to prevent gaining proximity to the bottom of the fence.

Spikes
The spikes would be in the top of a fence or wall to prevent scaling.

Privacy screening
Privacy screening can be slats or mesh fabric. It is used to limit visibility of any SAAs that may be on the other side of the fence.

Perimeter Security		
Other fence characteristics	Is there a clear zone? (An area inside or outside the perimeter that allows for clear sight of fence perimeter, e.g., no vegetation or objects, no privacy slats)	☐ No ☐ Yes
	Is the area free of objects / structures that would aid in traversing the fence (trees, sheds, barrels, etc.)	☐ No ☐ Yes *Describe:* _____
	Fence is clearly marked with visible, well-placed "warning" signs.	☐ No ☐ Yes
Perimeter Security - Fence Characteristics Comments: _____		
Overall Fence Comments: _____		

Other fence characteristics:

Is there a clear zone?
A clear zone should be an area both outside and inside the fence. It should be clear of vegetation.

Fence is clearly marked with visible, well-placed "warning" signs
Well-placed means that the signs are placed at intervals on the fence to clearly warn, not just at the entrance.

<table>
<tr><th colspan="3">Perimeter Security</th></tr>
<tr><td>Do Gates Exist?</td><td colspan="2">☐ No
☐ Yes</td></tr>
<tr><td>Gate Characterization (weakest of each type of gate)

☐ Vehicle</td><td>Style
☐ Hydraulic wedge
☐ Hydraulic Drop Arm
☐ Roller or Slide gate
☐ Swing gate
☐ Drop arm (not hydraulic)
☐ Moveable bollards
☐ Open/No gate

Additional Controls
☐ Sally Port (dual gates with entrapment area)
☐ Single Lane
☐ None

Characteristics
☐ Outriggers (e.g. barbed wire/razor wire)
☐ 45 degrees
☐ “Y” style
☐ Straight up
☐ None

Enhancements
☐ K-rated for vehicle penetration
☐ Privacy screening
☐ Coiled barbed wire
☐ Spikes
☐ Coiled razor wire
☐ None
Describe: _____</td><td>Construction
☐ Chain link
☐ Anti-climb Aluminum or Steel
☐ Standard Aluminum or Steel

☐ Other – not chain link
☐ Steel
☐ Wrought Iron
☐ Wood
☐ Plastic

Height
☐ Less than or equal to 5 ft.
☐ 5+ ft. - 6 ft.
☐ 6+ ft. – 7 ft.
☐ 7+1 ft. – 15 ft.
☐ Greater than 15 ft.

Gate is clearly marked with visible well-placed “warning” signs
☐ No
☐ Yes</td></tr>
<tr><td colspan="3">Vehicle Gate Briefing Notes: _____</td></tr>
</table>

Gate Characterization:
Select the types of gates that exist at the facility (vehicle, pedestrian and/or rail). You can select all three if applicable. Then select the style of gate for each type of gate, focusing on the weakest or least effective gate for each type. Similar to fencing, the focus should be on the weakest gate **that protects an SAA or entry to pertinent parts of the facility**. For example, the facility has four vehicle gates; however, one protects only the company baseball diamond, focus on the weakest of the other three. For instance, choosing between a wooden drop arm and a steel sliding gate, typically, the wooden drop arm is the weaker gate. Select the style for that weakest gate. Do the same for pedestrian and rail gates if it applies.

In another example, perhaps an emergency gate is really not accessible and breaching the gate on foot or with vehicle is not practical; then focus on the next weakest gate. You can add comments about all the other gates if desired.

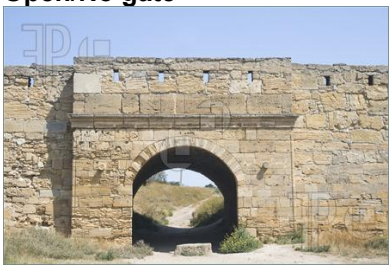
Style – Vehicle:

Hydraulic wedge

Hydraulic Drop Arm

Roller or Slide gate

Open/No gate



Swing gate

Drop arm (not hydraulic)

Moveable bollards

Sally Port (dual gates with entrapment area)

This page is intentionally left blank

Additional Controls

Single Lane
A gate where the road is narrowed down to allow only one lane of traffic at a time.

Characteristics:

Outriggers (e.g., barbed wire or razor wire)
It is assumed that the outriggers are equipped with a connecting wire such as barbed wire or razor wire. If they are not, they are not outriggers, but simply extra extensions on the end of the fence posts.

Enhancements:

K-rated for vehicle penetration
To select this option, the fence must have a verified DOS K-rating (4, 8, or 12).

Privacy screening
Privacy screening can be slats or mesh fabric. It is used to limit visibility of any SAAs that may be on the other side of the fence.

Coiled razor wire or coiled barbed wire
This can be additional razor or barbed wire coiled at the top of the fence within the regular outrigger or coiled at the bottom of the fence to prevent gaining proximity to the bottom of the fence.

Spikes
The spikes would be in the top of a fence or wall to prevent scaling.

Anti-Climb Aluminum or steel
Anti-climb includes mesh chain link or any type of aluminum or steel fence that has a very small opening that makes it more difficult to climb or cut. Often this fence has openings in the mesh of 1 inch or less as compared to standard chain link that normally has openings of about 2 inches.

Characteristics:
Outriggers (e.g., barbed wire or razor wire)
It is assumed that the outriggers are equipped with a connecting wire such as barbed wire or razor wire. If they are not, they are not outriggers, but simply extra extensions on the end of the fence posts.

Enhancements:

K-rated for vehicle penetration
To select this option, the fence must have a verified DOS K-rating (4, 8, or 12).

Privacy screening
Privacy screening can be slats or mesh fabric. It is used to limit visibility of any SAAs or facility that may be on the other side of the gate.

Anti-Climb Aluminum or steel
Anti-climb includes mesh chain link or any type of aluminum or steel chain link that has a very small opening that makes it more difficult to climb or cut. Often this fence has openings in the mesh of 1 inch or less as compared to standard chain link that normally has openings of about 2 inches.

Coiled razor wire or coiled barbed wire
This can be additional razor or barbed wire coiled at the top of the gate within the regular outrigger or coiled at the bottom of the gate (very unusual) to prevent access to the bottom of the gate.

Spikes
The spikes would be in the top of a gate to prevent scaling of the gate by a person.

Perimeter Security		
☐ Pedestrian	**Style** ☐ Full Height turnstile ☐ Swing gate ☐ Open turnstile ☐ Open/No gate **Characterization** ☐ Outriggers (e.g., barbed wire/razor wire) ☐ 45 degrees ☐ "Y" style ☐ Straight up ☐ None **Enhancements** ☐ Reinforced anchor points ☐ Coiled razor wire ☐ Coiled barbed wire ☐ Spikes ☐ None *Describe:* _____	**Construction** ☐ Chain link ☐ Anti-climb Aluminum or Steel ☐ Standard Aluminum or Steel ☐ Other – not chain link ☐ Steel ☐ Wrought Iron ☐ Wood ☐ Plastic **Height** ☐ Less than or equal to 5 ft. ☐ 5+ ft. - 6 ft. ☐ 6+ ft. – 7 ft. ☐ 7+ ft. – 15 ft. ☐ Greater than 15 ft. Gate is clearly marked with visible well-placed "warning" signs ☐ No ☐ Yes
Pedestrian Gate Briefing Notes: _____		

Style – Pedestrian

Full Height turnstile

Swing gate

Open turnstile

Perimeter Security		
☐ Rail	**Style** ☐ Moveable bollard/jersey ☐ Roller or Slide gate ☐ Swing gate ☐ Drop arm ☐ Open/No gate **Additional Controls** ☐ Sally Port (dual gates with entrapment area) ☐ Single Track ☐ None **Characterization** ☐ Outriggers (e.g., barbed wire or razor wire) ☐ 45 degrees ☐ "Y" style ☐ Straight up ☐ None **Enhancements** ☐ Train derailer ☐ Coiled razor wire ☐ Coiled barbed wire ☐ Spikes ☐ None *Describe:* _____	**Construction** ☐ Chain link ☐ Anti-climb Aluminum or Steel ☐ Standard Aluminum or Steel ☐ Other – not chain link ☐ Steel ☐ Wrought Iron ☐ Wood **Height** ☐ Less than or equal to 5 ft. ☐ 5+ ft. 6 ft. ☐ 6+ ft. – 7 ft. ☐ 7+ ft. – 15 ft. ☐ Greater than 15 ft. Gate is clearly marked with visible well-placed "warning" signs ☐ No ☐ Yes
Rail Gate Briefing Notes: _____		
Overall Gate Comments: _____		

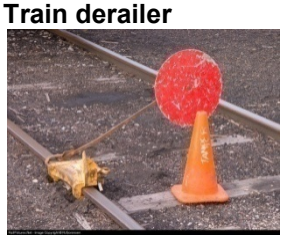
Rail Gates

Sally Port (dual gates with entrapment area)

Characteristics:
Outriggers (e.g., barbed wire or razor wire)
It is assumed that the outriggers are equipped with a connecting wire such as barbed wire or razor wire. If they are not, they are not outriggers, but simply extra extensions on the end of the fence posts.

Enhancements

Train derailer



Coiled razor wire or coiled barbed wire
This can be additional razor or barbed wire coiled at the top of the fence within the regular outrigger or coiled at the bottom of the fence to prevent gaining proximity to the bottom of the fence.

Spikes
The spikes would be in the top of a fence or wall to prevent scaling.

Anti-Climb Aluminum or steel
Anti-climb includes mesh chain link or any type of aluminum or steel fence that has a very small opening that makes it more difficult to climb or cut. Often this fence has openings in the mesh of 1 inch or less as compared to standard chain link that normally has openings of about 2 inches.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
Facility or SAA does not allow or does not receive these individuals or groups (not open to the public, no customers, no visitors)				
Unattended, no personnel involved in access to the facility or SAA (go to locks and technology)				
Entry Control Personnel During Operating Hours Briefing Notes: _____				

ENTRY CONTROLS

There are several entry control help videos available on IST Help.

For Entry Controls, consider the entry controls in place during operating hours and then again for off-business hours. Operating hours is for the facility during regular facility operations, including when the facility is open to the public (including during game day/incident day at a sports/event venue), carrying on full operations or for unmanned facilities when employees, contractors or visitors would normally enter the facility. Off-business hours are the times when the facility is either closed with no operations or operating in a reduced mode that changes the security posture. If the facility is a 365/24/7 facility, you may indicate that the entry controls are the same for both business hours and non-operating hours to cover all 24 hours of the day. It is often helpful to consider the entry control elements as statements that either apply or do not apply. It is also best to answer by column, verses row. Others have discovered it is best just to ask about the process without displaying the actual section (for those who tend to display the question set).

Next determine the types of individuals that are allowed into the facility. Each type of individual may have different entry controls. For each type of individual entering the facility, select the weakest controls imposed by the facility. So, if one gate has a swipe card only and one gate has an armed guard that checks the employee ID, complete the entry controls at the weakest employee entrance. Similarly complete the controls for the weakest visitor entrance, weakest contractor entrance and weakest patron/customer entrance. Include all entry controls that must be utilized to get to the actual facility or SAAs. For instance, if a visitor must first enter the lobby and receive a badge, go up in the elevator and then be admitted by an unarmed guard and then be escorted while within the facility, all of these entry controls should be selected not just the first “hurdle” the visitor must pass. During an SAV, some SAAs may have more layers of entry control than others. For an SAV select the weakest entry control layers to enter the facility or SAA.

There are four categories of facility entry control: Employee, Visitor, Contractor/Vendor, and Customer / Patron / Public.

Employee is defined as individuals that work for that particular facility. If you were to look at their pay statement it would clearly state they are employed directly by company XYZ. This does not include contractor/vendor regardless of how integrated the contractor is into the company. All facilities will have employees there at some point in time and entry controls should always be completed for employees.

Visitor is defined as an individual that is normally not employed by the facility and is visiting the facility to conduct business, attend meetings, go on a facility tour or has some reason to see an employee or employees at the facility. It is possible, yet very rare, that a visitor could be an employee of the facility, but is from a different location. For example, a Company ABC employee that is assigned to a Seattle office visits the Chicago office. The only reason this example would apply is if the visiting employee (from Seattle) has to go through a different access control process at the Chicago office than the employees assigned to the Chicago office.

Contractor / Vendor is defined as anyone who comes to the facility for the purposes of conducting work such as maintenance, construction, security, refill candy machines, soda machines, deliver materials or a host of other reasons. This category also includes contractors that are employed by the facility directly and may work side by side with the regular employees of the facility. For example, a Company ABC employee that is contracted by Company XYZ and works at the Chicago office. The access control process of the contractor may be identical to the regular employee, or may be slightly different. This also includes a security force that is contracted such as Wackenhut or Securitas who may provide various levels of security for a facility. However, the contractor/vendor that is given access to the facility/SAA with the weakest control should be the focus of the answers for this section (e.g., the candy machine vendor).

This page is intentionally left blank

Customer / Patron / Public is limited to any situation where the facility/SAA is open to the public and individuals are invited into the facility. Shopping malls, museums, arenas, stadiums, parks, theaters, and retail facilities are all examples where a customer or patron is likely to be found. This also applies to facilities such as a State driver license facility that people must visit to get a license and similar types of facilities. A road bridge is typically open to the public, since the public may drive their cars across the bridge. (However, be sure to identify under contractor the access control for the person conducting preventive maintenance on the bridge). A railroad bridge is normally not open to the public. Even though people can access the bridge, since the rail lines must be kept clear for trains, in most cases, people on rail lines or tracks would be considered trespassing.

It is assumed trespassing can occur anywhere, but these individuals are not visitors or customers/patrons/public. The entry controls in place are assumed to be the facility's attempt to prevent trespassers.

If the facility is open to the public, the column for patrons/customers will apply. Open to the public is a facility that invites the public to enter, e.g., stadiums, museums, shopping malls, or hotels. If the facility is not open to the public, select "Facility or SAA does not allow or does not receive these individuals or groups (not open to the public, no customers, no visitors)" and no entry controls need to be selected for that type of individual.

If facilities do not allow visitors or contractors, select "Facility or SAA does not allow or does not receive these individuals or groups (not open to the public, no customers, no visitors). This selection is not allowed for employees (grayed out or no checkbox). There are some facilities that do not receive visitors at all. Only facilities open to the public will probably have customers or patrons. There are very few facilities that do not receive contractors or vendors. If this selection applies, no entry controls need to be selected for that type of individual. In the electronic version, this column will blank out once this selection is checked. This selection must be checked once for business hours section and again for entry controls during off-business hours. For instance, patrons/customers/public or contractor/vendors may be allowed during business hours, but not at all during off-business hours.

If entry does not involve getting past a person, e.g., an employee door with a swipe card or a perimeter gate with a padlock, indicate that entry is "Unattended, no personnel involved in access to the facility or SAA and go directly to the locks and technology section.

Entry controlled by personnel has two sections, face-to-face contact/control and through a remote control device. If the facility has both types of entry control, complete both sections.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
People (face to face interaction, not remote camera or call box)				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
Guard (armed)				
Guard (unarmed)				
Employee that is not a security guard but controls access				
Ticket or toll collection agent				
Entry Control Personnel During Operating Hours Briefing Notes: _____				

People (face to face interaction, not remote camera or call box)

Employee that is not a security guard but controls access can be a receptionist if his/her job is to implement any of the controls listed below. This can include casual recognition in that the receptionist would report someone entering that is not recognized. If it is a person that has no entry control duties and is simply there to point people in the correct direction or answer questions, do not select this type of face-to-face entry.

Ticket or toll collection agent would only apply to patrons/customers at a facility open to the public. Even though this is not a strict type of entry control, it is something that would allow the personnel controlling entry to stop someone from entering without taking some action and thus allowing entry control personnel to report improper entry to the facility or SAA.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
People (remote camera or call box of some type)				
Guard (security force, armed or unarmed) with validation (e.g., visitor list)				
Employee that is not a security guard with validation (e.g., visitor list)				
Call button or camera that is acknowledged without validation. (Buzz them in without knowing who it is)				
Entry Control Personnel During Operating Hours Briefing Notes: _____				

People (remote camera or call box of some type)

Guard (security force, armed or unarmed) with remote camera and validation (e.g., visitor list)
Guard with remote camera and validation means the guard looks through the camera and validates the visitor (e.g., checks some list or documentation) before remotely allowing the visitor/contractor/employee to enter the facility.

Guard (security force, armed or unarmed) without remote camera but with validation (e.g., visitor list)
Guard does not have a remote camera, but through the call box validates the visitor (e.g., checks some list or documentation) before remotely allowing the visitor/contractor/employee to enter the facility.

Employee that is not a security guard granting access with remote camera and validation (e.g., visitor list)
Employee with remote camera and validation means that the person activating the entry control device checks some list or documentation before remotely allowing the visitor/contractor/employee to enter the facility. This could be a receptionist or an employee being visited. For instance, a call box that allows a visitor or contractor to dial a number of the person they are there to see and be admitted after identifying themselves through the device.

Employee that is not a security guard granting access without remote camera but with validation (e.g., visitor list)
Employee does not have a remote camera, but through the call box validates the visitor (e.g., checks some list or documentation) before remotely allowing the visitor/contractor/employee to enter the facility. This could be a receptionist or an employee being visited. For instance, a call box that allows a visitor or contractor to dial a number of the person they are there to see and be admitted after identifying themselves through the device.

Call button or camera that is acknowledged without validation. (Buzz them in without knowing who it is)
This is the weakest entry control and would allow anyone, without any validation as to identity or purpose to enter the facility with the simple activation of the remote device.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
Process that requires a person be present to implement				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
X-Ray Scanner				
Escort required at all times				
Escort required only in sensitive areas				
Metal Detectors (Magnetometer)				
Vapor Detectors				
Chemical Detectors				
Ion Mobility Spectrometer				
Radiation Detection				
Exchange badge				
Credential check (Facility issued photo ID)				
Credential displayed while onsite				
Credential designates access to specific areas				
Canine Olfaction (K-9)				
Package Searches				
Physical Searches				
Credential check (Facility issued non-photo ID)				
Credential check (Gov. issued ID)				
Sign in / out				
Casual Recognition				
Entry Control Process During Operating Hours Briefing Notes: _____				

Process that requires a person be present to implement
The following entry controls can only be selected if it is indicated that a person is present to implement those controls. For instance you cannot have a metal detector or vapor detector without a person to monitor the procedure.

X-Ray Backscatter Scanner
Low-dose scanning devices that safely examine people for hidden items, providing an image of the body beneath clothes.

Metal Detectors (Magnetometer)
People or packages are made to pass through metal detector/magnetometer.

Vapor Detectors
A swipe sample can be collected and heated to vaporize particles from the sample or an air sample can be collected. The vapor is then analyzed to detect trace explosives vapors.

Chemical Detectors
These devices may be electric or non-electric. They range from air samplers to wipes of some type to sophisticated electronic devices that identify particulates.

Ion Mobility Spectrometer
A spectrometer capable of detecting and identifying very low concentrations of chemicals based upon the differential migration of gas phase ions through a homogeneous electric field.

Radiation Detection
A device that can detect radiation (e.g., Geiger counters, dosimeters)

Exchange badge
This is where the personnel badge is not taken home, but something must be provided before the badge is re-issued to the employee each day (e.g., a driver's license).

Credential check (Facility issued photo ID)
This is where the Guard/entry personnel require a facility-issued photo ID be presented prior to entry.

Credential designates access to specific areas
This would require that the badge has some distinguishing attribute (e.g., color or words) to indicate the areas where the person wearing the badge is to have access

Canine Olfaction (K-9)
This is the use of dogs to detect contraband on persons or in packages.

Package Searches
Incoming packages are passed through an X-ray technology device that produces an image for an operator to inspect.

Physical Searches
Guards/personnel search people entering the building for contraband

Credential check (Facility issued non-photo ID)
This is where the Guard/entry personnel require a facility-issued ID with no photo be presented prior to entry.

Credential check (Gov. issued ID)
This is where the guard/entry personnel require a government-issued ID (e.g., driver's license) prior to entry.

Sign in / out
Individuals entering the facility/SAA are required to sign in upon entry and sign out when leaving.

Casual Recognition
This is where the guard/entry personnel simply recognize employees or vendors to allow entry to the facility.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
Locks and Technology Identify the locks and technology in place to control access.				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
Biometric (hand, eye, signature, voice, face)				
ID actuated (coded credential, proximity card, swipe card)				
Electronically coded (PIN)				
Mechanically coded (PIN)				
Key cylinder lock (door mounted)				
Combination lock (door mounted)				
Padlock/chain or hasp				
No locks or technology controls at any time				

Identify the locks and technology in place to control access
The answers below should reflect the weakest entry control point at the facility/SAA. It may reflect layers of security in that it should include each type of lock that is necessary to get into the facility. So, if all employees use a swipe card to enter the facility, but there are additional locks to access specific SAAs, for the facility only ID actuated would be selected. However, if entry to the SAA, which is the data control room, entry control locks and technology may include a lock at the lobby of the building, the lock (swipe card) in the elevator (facility controls), and the lock on the data center door (SAA only).

Biometric (hand, eye, signature, voice, face)
Where entry depends on personnel identity verification systems that corroborate claimed identifies on the basis of some unique physical biometric characteristic, including hand or finger geometry, handwriting, eye pattern, fingerprints, speech, fact and various other physical characteristics. Biometric devices can differentiate between verification and recognition. In verification mode, a person initiates a claim of identity, presents the specific biometric feature for authorization and the equipment agrees. In recognition mode, the person does not initiate the claim, the biometric devices attempts to identify the person and the biometric information is compared with a database.

ID actuated (coded credential, proximity card, swipe card)
This is typically considered some type of lock that requires other identification before the lock is activated. This may be some type of swipe card, badge activation. If this option is selected, please provide information on additional access control activities.

Electronically coded (PIN)
This is a random generated keypad attached to the door/gate.

Mechanically coded (PIN)
This is a cipher lock keypad attached to the door/gate.

Key cylinder lock (door mounted)
This is a normal door lock activated with a key.

Combination lock (door mounted)
This is a combination lock mounted on the door/gate. This does not include padlocks activated with a combination. If this option is selected, please provide information on additional access control activities.

Padlock/chain or hasp
This is a typical padlock that can be activated by a key or combination that is latched through a hasp attached to the door or gate or through a chain that secures the door/gate to the accompanying fence or wall so that the door/gate cannot be opened sufficiently to allow entry. If this option is selected, please provide information on additional access control activities.

No locks or technology controls at any time
This may be an appropriate selection for a contractor, vendor, visitor or customer if it has been selected that the person is always escorted, since they will not be provided their own technology control or keys, but will rely on the escort to activate any locks or technology controls.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
Locks and Technology Identify the locks and technology in place to control access.				
If key-actuated lock (door mounted) or Padlock/chain or hasp is selected, additional access control activities for systems				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
System exists for retrieving keys from terminated employees and contractors				
Formal key control inventory are in place (who has what key)				
Keys cannot be easily duplicated				
Master keys are not used outside of the security force				
None (Facility uses keys, no key control system)				

If key-actuated lock is selected, additional access control activities for systems
This section would be completed ONLY IF the facility uses key-cylinder locks for its weakest doors/gates or Padlock/chain or hasp.

System exists for retrieving keys from terminated employees and contractors
This is a system that uses the key inventory to determine which terminated employees or contractors have critical keys and identifies a process for retrieving those keys before the terminated individual leaves the facility. Termination can be either voluntary or involuntary.

Formal key control inventory are in place (who has what key)
A formal key control inventory must have procedures to determine what keys are to critical areas or assets; determine who has each such key, including a process for periodically auditing key assignment to make sure each key is accounted for.

Keys cannot be easily duplicated
These are usually keys that have unusual key blanks such that the local True Value will not have a convenient blank for duplication. In addition, it is prudent to mark such keys with “Do Not Duplicate.”

Master keys are not used outside of the security force
It may be that maintenance and housekeeping has master keys to areas that are not secured or critical, however, to answer yes for this question, master keys to secure areas would be limited to security force/management.

Entry Controls				
ENTRY CONTROL DURING OPERATING HOURS How is access to the facility or SAA controlled when the facility is open such as during normal business hours, fully operational, normal staffed, or during event hours?				
Locks and Technology Identify the locks and technology in place to control access.				
If ID actuated lock is selected, additional access control activities for systems				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
System exists for removing termed or terminated employees from database				
Multiple access levels are in place based on need				
Entry control alarm and event activity is continuously monitored by a person				
Required to badge in and out				
Anti-passback				
No "piggy backing" policy				
Access card database is regularly reviewed for accuracy				
Access activity reports are reviewed regularly				
Fail secure				
Fail safe				
Entry Control Locks and Technology During Operating Hours Briefing Notes: _____				
Overall Entry Control During Operating Hours Comments: _____				

If ID actuated lock is selected, additional access control activities for systems
This section would be completed ONLY IF the facility uses ID-actuated locks for its weakest door/gate. ID-actuated may include swipe cards, proximity cards, and other items that electronically control entry using a device based on employee identity.

System exists for removing termed or terminated employees from database
This is a system that uses the ID card database to determine which terminated employees or contractors have ID-actuated swipe cards/keys and identifies a process for retrieving those keys before the terminated individual leaves the facility. Termination can be either voluntary or involuntary.

Multiple access levels are in place based on need
This is a process that allows the ID-actuated card/key to be activated only for certain zones or areas within the facility. For instance some employees can swipe only into the main gate, while others can swipe into secure areas and some into even more secure rooms.

Entry control alarm and event activity is continuously monitored by a person

Required to badge in and out
A card swipe in the device is needed to entry and to exit the facility.

Anti-passback
The goal or process in place should prevent a cardholder from passing back their pass or swipe card to gain entry to an access controlled area. There should be a physical barrier or person that prevents an individual from handing a pass or swipe card back to another person.

No "piggy backing" policy
Piggybacking is when one person uses their card in the device to access the facility and allows others to come in without using a card in the device. A “No piggybacking” policy requires each person to use their card in the device to gain access to the facility.

Access card database is regularly reviewed for accuracy
This is the process where ID-actuated cards are matched to employees and any discrepancies are corrected such that each card is correctly inventoried to a particular employee.

Access activity reports are reviewed regularly
This is a process where database reports of who is using which card where is reviewed to determine that the systems is correctly allowing entry only to properly issued cards and to ensure the system correctly limits access to areas with limited card access controls.

Fail secure
This is the situation where the door locks when power is removed and unlocks when power is restored.

Fail safe
This is the situation where if the electrical power fails, the door unlocks.

Entry Controls				
ENTRY CONTROL DURING OFF-BUSINESS HOURS How is access to the Facility or SAA controlled when the facility is closed, such as times when it has minimal staff, weekends, non-business hours or non-event hours				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
No change from ENTRY CONTROL DURING OPERATING HOURS. Access control process and procedures are the same regardless of operational status, operating hours, staffing or event				
Facility or SAA does not allow or does not receive these individuals or groups during off-business hours				
If the process changes, identify the differences by selecting the appropriate areas below				
Unattended, no personnel involved in access to the facility or SAA (move to locks and technology)				
People (face to face interaction, not remote camera or call box)				
Guard (armed)				
Guard (unarmed)				
Employee that is not a security guard but controls access				
Ticket or toll collection agent				
People (remote camera or call box of some type)				
Guard (security force, armed or unarmed) with validation (e.g., visitor list)				
Employee that is not a security guard with validation (e.g., visitor list)				
Call button or camera that is acknowledged without validation. (Buzz them in without knowing who it is)				
Entry Control Personnel During Off-business Hours Briefing Notes: _____				

No change from ENTRY CONTROL DURING OPERATING HOURS. Access control process and procedures are the same regardless of operational status, operating hours, staffing or event.
If the facility is open 365/24/7, and if there is no change to the control process and procedures for a type of individual gaining entry to the facility, just check this selection for each type of individual that enters the facility and no further selections need be reviewed (it will gray out in the web-based version, but just ignore them in the hard-copy version).

If, however, the control process or procedures changes during off-hours for any of the different types of individuals entering the facility, do not check this selection, but instead go through and select those control items that apply to that type of individual during this time of day for the facility. For instance, during the day employees go through the front gate and show their ID at the door, however, during off-business hours, employees would use a swipe card to enter through another door (perhaps not all employees, but those provided with this special access control device). Another example is a railroad station that is completely open during the busy hours of the day, but controls access during the night hours to allow only people with tickets for late-night train departures.

Entry Controls				
Process that requires people be present to implement				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public**
X-Ray Scanner				
Escort required at all times				
Escort required only in sensitive areas				
Metal Detectors (Magnetometer)				
Vapor Detectors				
Chemical Detectors				
Ion Mobility Spectrometer				
Radiation Detection				
Exchange badge				
Credential check (Facility issued photo ID)				
Credential displayed while onsite				
Credential designates access to specific areas				
Canine Olfaction (K-9)				
Package Searches				
Physical Searches				
Credential check (Facility issued non-photo ID)				
Credential check (Gov. issued ID)				
Sign in / out				
Casual Recognition				
Entry Control Process During Off-Business Briefing Notes: _____				

Entry Controls				
Identify the locks and technology in place to control access.				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public [Open to the public]**
Biometric (hand, eye, signature, voice, face)				
ID actuated (coded credential, proximity card, swipe card)				
Electronically coded (PIN)				
Mechanically coded (PIN)				
Key cylinder lock (door mounted)				
Combination lock (door mounted)				
Padlock/chain or hasp				
No locks or technology controls at any time				
If key-actuated lock (door mounted) or Padlock/chain or hasp is selected, additional access control activities for systems				
System exists for retrieving keys from terminated employees and contractors				
Formal key control inventory are in place (who has what key)				
Keys cannot be easily duplicated				
Master keys are not used outside of the security force				
None (Facility uses keys, no key control system)				

This page is intentionally left blank

Entry Controls				
If yes to ID-actuated lock, additional access control activities or systems				
	Employee	**Visitor**	**Contractor / Vendor**	**Customer / Patron / Public [Open to the public]**
System exists for removing termed or terminated employees from database				
Multiple access levels are in place based on need				
Entry control alarm and event activity is continuously monitored by a person				
Required to badge in and out				
Anti-passback				
No "piggy backing" policy				
Access card database is regularly reviewed for accuracy				
Access activity reports are reviewed regularly				
Fail secure				
Fail safe				
Entry Control Locks and Technology During Operating Hours Briefing Notes: _____				
Overall Entry Control During Operating Hours Comments: _____				

Parking/Delivery/Standoff		
Can any vehicle be placed (legally or illegally) within 400 feet of the facility or any SAA?	☐ No ☐ Yes If yes, is parking: ☐ Uncontrolled ☐ Controlled	
If yes, complete the following for parking controlled and/or uncontrolled. If there is no controlled parking, just complete for uncontrolled.		
	Controlled	**Uncontrolled**
Select the closest vehicle/vessel placement to the facility or SAA	☐ Company vehicle parking/Employee vehicle ☐ Legal public parking ☐ Delivery vehicle	☐ Company vehicle parking/delivery/docking ☐ Legal public parking ☐ Delivery vehicle ☐ Illegally placed vehicle
Select the largest-size of vehicle at this closest placement area to the facility or SAA.	☐ Car ☐ Van ☐ Truck (up to 26 feet) ☐ Truck (26 feet or more) ☐ Rail car ☐ Boat (30 feet or more) ☐ Ship/Barge	☐ Car ☐ Van ☐ Truck (up to 26 feet) ☐ Truck (26 feet or more) ☐ Rail car ☐ Boat (30 feet or more) ☐ Ship/Barge
Select the type of placement	**Type** ☐ Adjacent multi-level garage ☐ Adjacent on street ☐ Adjacent open lot ☐ Adjacent loading dock or pier ☐ Under building or structure ☐ Above building or structure (roof or similar situation)	**Type** ☐ Adjacent multi-level garage ☐ Adjacent on street ☐ Adjacent open lot ☐ Adjacent loading dock or pier ☐ Under building or structure ☐ Above building or structure (roof or similar situation)
Is parking/vehicle placement monitored?	☐ No ☐ Yes If Yes, parking is monitored by (check all that apply): ☐ CCTV ☐ 24/7 ☐ Security personnel ☐ 24/7 ☐ Other than security personnel ☐ 24/7	☐ No ☐ Yes If Yes, parking is monitored by (check all that apply): ☐ CCTV ☐ 24/7 ☐ Security personnel ☐ 24/7 ☐ Other than security personnel ☐ 24/7

PARKING/DELIVERY/STANDOFF

The concept for data collection in this section is to capture the largest vehicle that can get closest to the facility/SAA with the least controls. Therefore, a car within 10 feet with reasonable controls is less of a vulnerability to the facility than a car within 20 feet with no controls, even though it is closer. Conversely, a car within 10 feet within only minimal control (e.g., casual recognition) will be more vulnerability than a car within 20 feet with no controls. This section also addresses illegally-placed vehicles, not just legal parking.

This question determines whether the consequence of an explosion from a VBIED can be mitigated by increasing the distance a VBIED can be placed from the facility. This is also captured in calculation of the Protective Measures Index to capture preventing a VBIED from approaching the facility.

Can any vehicle be placed (legally or illegally) within 400 feet of the facility or any SAA?
If the only parking allowed is more than 400 feet from the facility or an SAA, it can be considered no parking is allowed at the facility.

Uncontrolled
This is parking that can be accessed by anyone without passing through any entry control point.

Controlled
Controlled parking is where the vehicle must get past some entry control point, attended or unattended.

Company vehicle parking
A company vehicle is a vehicle owned or leased by the facility owner/operator and operated by company personnel. It is usually placarded with the name of the company.

Employee vehicle parking
This refers to onsite employee parking (privately-owned vehicles).

Legal public parking
Legal parking can be on or off facility property, including employee parking, third-party parking (e.g., visitors or customers), nearby/adjacent public parking lots, and on-street parking.

Delivery vehicle
This can be any third-party (non-company) delivery vehicle making a delivery to the facility, including a facility dock, the building lobby, a chemical tank, or to the front door.

Illegally placed vehicle
An illegally-placed vehicle is one that can be parked on or off facility property, even though parking is not allowed (e.g., under a bridge with no-trespassing signs or in an alley with no-parking signs). It does not include ramming a fence to place the vehicle.

Parking/vehicle placement is monitored
Monitoring can include viewing the parking area (legal or illegal) on CCTV, via security personnel onsite or via other non-security personnel (e.g., parking attendants or onsite operations personnel)

Parking/Delivery/Standoff		
Is there a procedure/policy to identify and act on unauthorized extended-stay vehicles (e.g., reporting to security, LLE or tow company)?	☐ No ☐ Yes	☐ No ☐ Yes
What is the minimum standoff between vehicle and the facility or the nearest SAA?	Number of feet: _____	Number of feet: _____
Parking/Delivery/Standoff Briefing Notes: _____		
Overall Parking/Delivery/Standoff Comments: _____		

What is the minimum standoff between vehicle and the facility or the nearest SAA?
Consider where the main facility or any SAAs are located and the closest area where this closest uncontrolled parking is located. If you have on-street parking at a high-rise and no parking structure associated with the high-rise, the width of the sidewalk is your minimum standoff. When considering commercial buildings and the "facility" or the SAA is on an upper floor, if a VBIED within a parked vehicle can cause the destruction of the building, and thus the SAA or "facility," then the closest point for calculating minimum stand-off, should be the closest point parking is allowed next to the building.
Enter a single number to answer the minimum standoff question, even if it is 0. For instance, if there is under-building parking, the minimum standoff from the building is 0 feet.

Parking/Delivery/Standoff		
COMPLETE ONLY FOR CONTROLLED PARKING		
	During Business/Operating Hours	**During Off-Business/Operating Hours**
		Facility or SAA does not allow controlled parking during off-business/operating hours ☐ **Yes** ☐ **No** **If No, stop.**
		If yes, is there a change in parking access control for off-business hours? ☐ **Yes** ☐ **No** **If No, stop.**
If the facility allows controlled parking during these hours,	☐ Unattended, no personnel involved in the vehicle access to the facility or SAA (go to locks and technology) ☐ Attended	☐ Unattended, no personnel involved in the vehicle access to the facility or SAA (go to locks and technology) ☐ Attended
***If attended*, personnel-controls at the weakest parking access control point:**		
Access controlled by face-to-face personnel interaction:		
Guard (armed)	☐	☐
Guard (unarmed)	☐	☐
Employee that is not a security guard but controls access	☐	☐
Ticket or toll collection agent	☐	☐
Access controlled by person but via remote CCTV or call box of some type		
Guard (security force, armed or unarmed) with validation (e.g., visitor list)	☐	☐
Employee that is not a security guard with validation (e.g., visitor list)	☐	☐
Call button or camera that is acknowledged without validation. (Buzz them in without knowing who it is)	☐	☐
***If attended,* weakest parking access vehicle search**		
Vehicle Search	☐	☐
100%	☐	☐
Random	☐	☐

Is there a change in parking/delivery access control for off-business hours?
For Facility Entry Controls, consider the entry controls in place during operating hours and then again for off-business hours. Operating hours is for the facility during regular facility operations, including when the facility is open to the public (including during game day/incident day at a sports/event venue), carrying on full operations or for unmanned facilities when employees, contractors or visitors would normally enter the facility. Off-business hours are the times when the facility is either closed with no operations or operating in a reduced mode that changes the security posture. If the facility is a 365/24/7 facility, you may indicate that the entry controls are the same for both business hours and non-operating hours to cover all 24 hours of the day.

Entry controlled by personnel has two sections, face-to-face contact/control and through a remote control device.
Access controlled by face-to-face personnel interaction:
Employee that is not a security guard can be a parking attendant or other type of employee if his/her job is to implement any of the controls listed below. If it is a person that has no entry control duties and is simply there to point people in the correct direction or answer questions, do not select this type of face-to-face vehicle control.
Ticket or parking fee collection agent would only apply to patrons/customers at a facility open to the public. Even though this is not a strict type of vehicle entry control, it is something that would allow the personnel controlling entry to stop someone from entering without taking some action and thus allowing vehicle entry control personnel to report improper vehicle entry to the facility or SAA.

Access controlled by person but via remote CCTV or call box of some type:
Guard (security force, armed or unarmed) with validation (e.g., visitor list): Guard with validation means the guard validates the driver (e.g., checks some list or documentation) before remotely allowing the vehicle to enter the facility.

Employee that is not a security guard granting access with validation (e.g., visitor list): Employee with validation means that the person activating the entry control device checks some list or documentation before remotely allowing the vehicle to enter the facility. This could be a receptionist or an employee being visited. For instance, a call box that allows a driver to dial a number of the person they are there to see and be admitted after identifying themselves through the device.

Call button or camera that is acknowledged without validation. (Buzz them in without knowing who it is): This is the weakest entry control and would allow any vehicle, without any validation as to identity or purpose to enter the facility with the simple activation of the remote device.

If attended, weakest parking access vehicle search
The following entry controls can only be selected if it is indicated that a person is present to implement those controls. For instance you cannot have a metal detector or vapor detector without a person to monitor the procedure.

Vehicle Searches
Vehicle search may be simple visual surveillance of the vehicle interior, use of mirrors to check the underside of the vehicle, or other any other type surveillance to detect weapons, explosives or contraband inside a vehicle. The searches are either 100% or random. Random is when only certain vehicles are selected for search. This can be based on a criteria or a percentage (less than 100%).

Parking/Delivery/Standoff		
COMPLETE ONLY FOR CONTROLLED PARKING		
Type of Vehicle Search		
X-Ray Scanner	☐	☐
Metal Detectors (Magnetometer)	☐	☐
Vapor Detectors	☐	☐
Chemical Detectors	☐	☐
Radiation Detection	☐	☐
Canine Olfaction (K-9)	☐	☐
Visual	☐	☐
Locks and Technology Identify the locks and technology in place to control access to the parking area.		
Biometric (hand, eye, signature, voice, face)	☐	☐
ID actuated (coded credential, proximity card, swipe card)	☐	☐
Electronically coded (PIN)	☐	☐
Mechanically coded (PIN)	☐	☐
Key cylinder lock (door mounted)	☐	☐
Combination lock (door mounted)	☐	☐
Padlock/chain or hasp	☐	☐
No locks or technology controls at any time	☐	☐
Parking/Delivery Controls Briefing Notes: _____		
Overall Parking/Delivery Controls Comments: _____		

X-Ray Scanner
Low-dose scanning devices that safely examine people for hidden items, providing an image of the body beneath clothes.

Radiation Detection
A device that can detect radiation (e.g., Geiger counters, dosimeters)

Canine Olfaction (K-9)
This is the use of dogs to detect contraband on persons or in packages.

Metal Detectors (Magnetometer)
People or packages are made to pass through metal detector/magnetometer.

Chemical Detectors
These devices may be electric or non-electric. They range from air samplers to wipes of some type to sophisticated electronic devices that identify particulates.

Locks and Technology

Identify the locks and technology in place to control access
The answers below should reflect the weakest entry control point at the facility/SAA. It may reflect layers of security in that it should include each type of lock that is necessary to get to the facility/SAA. For instance, if entry to the facility, which is floors 7-10 of a tall building, may include a lock at the lobby of the building, the lock (swipe card) in the elevator, and the lock on the facility floor door.

Biometric (hand, eye, signature, voice, face)
Where entry depends on personnel identity verification systems that corroborate claimed identifies on the basis of some unique physical biometric characteristic, including hand or finger geometry, handwriting, eye pattern, fingerprints, speech, fact and various other physical characteristics. Biometric devices can differentiate between verification and recognition. In verification mode, a person initiates a claim of identity, presents the specific biometric feature for authorization and the equipment agrees. In recognition mode, the person does not initiate the claim, the biometric devices attempts to identify the person and the biometric information is compared with a database.

ID actuated (coded credential, proximity card, swipe card)
This is typically considered some type of lock that requires other identification before the lock is activated. This may be some type of swipe card, badge activation.

Electronically coded (PIN)
This is a random generated keypad attached to the door/gate.

Mechanically coded (PIN)
This is a cipher lock keypad attached to the door/gate.

Key cylinder lock (door mounted)
This is a normal door lock activated with a key.

Combination lock (door mounted)
This is a combination lock mounted on the door/gate. This does not include padlocks activated with a combination.

Padlock/chain or hasp
This is a typical padlock that can be activated by a key or combination that is latched through a hasp attached to the door or gate or through a chain that secures the door/gate to the accompanying fence or wall so that the door/gate cannot be opened sufficiently to allow entry.

<table>
<tr><th colspan="3">Barriers</th></tr>
<tr><td>Does the facility or SAA have a high-speed avenue(s) of approach?</td><td colspan="2">☐ No ☐ Yes</td></tr>
<tr><td>If yes, does the facility or SAA use barriers to mitigate a high-speed avenue of approach?</td><td colspan="2">☐ No ☐ Yes</td></tr>
<tr><td>Barriers Characterization

(Weakest barrier type at the facility/SAA to mitigate a high-speed avenue of approach)</td><td><u>Type</u>

☐ Bollards, planters or rocks
☐ Jersey barrier/wall
☐ Earthen berm
☐ Spike system/tire shredders
☐ Guard rails
☐ Natural barriers (e.g., trees)
☐ Maritime or water deployed (e.g., floating or boat barrier)</td><td><u>Characterization</u>

☐ K-rated
☐ Not K-rated</td></tr>
<tr><td colspan="3">High-speed Avenue of Approach Barrier Briefing Notes: _____</td></tr>
<tr><td>Does the facility use barriers to enforce standoff from the facility or SAA?</td><td colspan="2">☐ No ☐ Yes</td></tr>
<tr><td>Barriers Characterization

(Weakest barrier type at the facility/SAA used to provide standoff)</td><td colspan="2"><u>Type</u>
☐ Bollards, planters or rocks
☐ Jersey barrier/wall
☐ Earthen berm
☐ Spike system/tire shredders
☐ Guard rails
☐ Natural barriers (e.g., trees)
☐ Maritime or water deployed (e.g., floating or boat barrier)</td></tr>
<tr><td colspan="3">Standoff Barrier Briefing Notes: _____</td></tr>
<tr><td colspan="3">Overall Barrier Comments: _____</td></tr>
</table>

BARRIERS

Does the facility or SAA have a high-speed avenue(s) of approach?
A high-speed avenue of approach is any road or flat area that would allow a vehicle to gain sufficient speed to enter or reach the facility/SAA before the attack can be detected, deterred or interdicted. If a facility has installed traffic calming, road redirection, berms, or jersey barriers, to the extent that a high-speed avenue of approach is now mitigated, select "No". This indicates that while the facility or SAA may have once had that vulnerability, it is mitigated and no longer exists due to specific actions the facility has taken to solve that vulnerability. High-speed avenue of approach does not apply only to roads. For example: A high-speed avenue of approach still exists if an SAA is near the perimeter of a fenced facility. The fence is typical 6-foot chain link with no reinforcement or anchoring and is located at the end of a T intersection or easily traversed open area where it is common for vehicles to travel. A high speed avenue of approach may also still exists if a facility has installed barriers to create a serpentine or traffic calming, but they devices are placed in such a manner that the barriers can be avoided, are too far apart, are lightweight plastic barrels or cones that will not impede vehicle travel.

If yes, does the facility or SAA use barriers to mitigate a high-speed avenue of approach?
Barriers are fixed or movable objects of some type placed to mitigate or reduce the impact of a vehicle ramming an object (SAA), building, or going through a checkpoint, gate or other control point at high speed. A barrier in this case does not include jersey barriers installed to create a serpentine approach to an entrance or gate. If that traffic calming is in place, then the high-speed avenue of approach should not exist.

Type

Bollards, planters or rocks
Bollards are rigid posts that can be arranged in a line to close a road or path to vehicles. They can be made of concrete, metal, or wood. Planters are usually concrete “bowls” with flowers or plants in the center. They are heavy enough to stop or delay a high-speed vehicle. Rocks are large stones of sufficient weight to stop or delay a vehicle.

Jersey barrier/wall
Jersey barriers are usually made of concrete or plastic filled with an inert substance that were originally developed to ensure vehicles do not cross lanes of traffic, usually stand about three feet tall with sloping sides.

Earthen berm
An earthen berm is a mound of dirt of sufficient slope and height to slow or prevent a vehicle from making a high-speed approach to the facility or SAA.

Spike system/tire shredders
Spike system/Tire shredders puncture the tires of an intruding vehicle, while allowing passage of vehicles in the opposite direction.

Guard rails
Guard rails are effectively one strong band that transfers the force of the vehicle to multiple posts beyond the impact area or into a ground anchor at the end of the guardrail.

Natural barriers (e.g., trees)
This could be closely spaced large trees, river banks or other barriers that would not allow a vehicle to drive over or through it at high speed.

Maritime or water deployed (e.g., floating or boat barrier)
Usually this is an anchored, floating barrier that can encircle a vessel to prevent other vessels from coming within a specified distance.

This page is intentionally left blank

K-rated
The Department of State has issued standards for vehicle barriers. If a vehicle barrier must have been tested by an independent crash test facility to meet DOS standards.

These standards incorporate speed (K) and penetration. The test specifies perpendicular barrier impact by a 15,000 lb. (6810 kg.) vehicle. The standards have different certification classes based on speed. K12 is a 15,000 lb. vehicle at 50 mph; K8 is that vehicle at 40 mph and K4 is at 30 mph. To become certified with a Department of State "K" rating the 15,000 vehicle must achieve one of the K rating speeds (50 mph, 40 mph, or 30 mph) and the bed of the truck must not penetrate the barrier by more than 36 inches. Generally, if a facility has paid to have a K-rated barrier installed, it will know the K-rating since the certification is reflected in the price and installation.

Does the facility use barriers to enforce standoff from the facility or SAA?
This is when the facility uses barriers to prevent vehicles from parking closer to the facility than the location of the barriers. They may not be as robust as those installed at a high-speed avenue of approach to prevent a vehicle from ramming through a fence or gate.

Building Envelope	
Is the facility/SAA in a building?	☐ No ☐ Yes
Windows	
Does the facility/SAA have windows?	☐ No ☐ Yes
Are there ground floor windows (less than 18 feet from the ground) in the facility or the SAA?	☐ No ☐ Yes
If yes, are there protective measures on the ground floor windows for the facility or the SAA?	☐ No ☐ Yes
Characterize the protective measures on the weakest facility or SAA window(s)	If yes, ☐ Blast curtains ☐ Blast/safety film ☐ Bullet-proof glass ☐ Laminated glass ☐ Wire-reinforced glass ☐ Thermally-tempered glass (TTG)

BUILDING ENVELOPE

Is the facility/SAA in a building?
Remember the definition of the facility and the SAAs that have been selected. If a facility, such as a bridge, has enclosed spaces, but are not specifically buildings, select "No" to this question, however, you can discuss the entrances thereto later. Often an IST is conducted on a facility that has both buildings and areas in the open (e.g., wastewater treatment, open roof NFL stadium, refinery). When conducting the SAV, each SAA can be identified individually as being in a building or not. For the ECIP Survey, the facility must be taken as a whole and do not focus on a given SAA. The most common example is a wastewater facility where there are some buildings (considered as SAA's) that house the SCADA system and there are facilities (considered as SAA's) not in a building (ponds or tanks). In this case the ECIP Survey should answer that there is a building since it would make no sense to have a SCADA system (at least the process control unit) exposed to the environment. Use this same logic for the windows, doors, walls and ceiling.

Does the facility/SAA have windows?
The focus should be on the weakest windows **found in buildings that are the primary facility or that house an SAA**. For example, the facility may have impact resistant windows on most ground-floor windows, but in the building housing a SAA they have plain single pane glass. In this example, although the vast majority of the windows are excellent, the SAA protected by single pane windows creates a vulnerability and therefore are the windows on which the questions should focus and will be used for scoring purposes. If the facility/SAA is made of glass "walls" indicate that the building has windows. The purpose of this section is to determine whether the facility is vulnerable to the impact of a bomb explosion on glass.

Are there ground floor windows (less than 18 feet from the ground) in the facility or the SAA?
Although it is understood that windows above the ground floor are also susceptible to a bomb explosion, the section is concerned with the immediate effect on ground floor windows.

Characterize the protective measures on the weakest facility or SAA window(s)
Blast curtains
Protective apparatus including a plurality of spaced, slender tensile elements installed in a room inwards of a glass panel of a curtain wall of the room, wherein when the glass panel is destroyed by an explosive blast, the tensile elements generally prevent fragments from the glass panel from flying inwards past the tensile elements.

Blast/safety film
Fragment retention window films are designed to increase the shatter resistance of glass and are similar to regular window films in that they are polyester laminates. The difference, however, is that these products are usually thicker – offered in thicknesses ranging from 4 to 14mils – and use a heavier and more aggressive adhesive system.

Bullet-proof glass
Bullet-resistant glass (colloquially known as bulletproof glass) is a type of strong but optically transparent material that is particularly resistant to being penetrated when struck by bullets. Bullet-resistant glass is usually constructed using polycarbonate thermoplastic or layers of laminated glass. The aim is to make a material with the appearance and clarity of standard glass but with effective protection from small arms. Polycarbonate designs usually consist of products such as ArmorMax, Makroclear, Cyrolon, Lexan or Tuffak, which are often sandwiched between layers of regular glass.

This page is intentionally left blank

Laminated glass
Laminated glass is a type of safety glass that holds together when shattered. In the event of breaking, it is held in place by an interlayer, typically of polyvinyl butyral (PVB), between its two or more layers of glass. The interlayer keeps the layers of glass bonded even when broken, and its high strength prevents the glass from breaking up into large sharp pieces. This produces a characteristic "spider web" cracking pattern when the impact is not enough to completely pierce the glass.

Wire-reinforced glass
Wire-reinforced glass is glass that has been reinforced with wire. Certain building codes require safety glass in specific situations. The wire within the pane keeps the glass shatterproof even at very high temperatures.

Thermally-tempered glass (TTG)
Tempered glass is glass that has been processed by controlled thermal or chemical treatments to increase its strength compared with normal glass

Building Envelope	
Doors	
Does the facility/SAA have doors?	☐ No ☐ Yes
Characterize the construction of the weakest door that provides access to the facility or SAA	☐ Blast resistant ☐ Metal-clad ☐ Hollow-steel ☐ Fire-rated door ☐ Wood, hollow core ☐ Wood, solid core ☐ Metal or wooded framed glass (at least 50% of the door is glass) If present: ☐ Interior or concealed hinges ☐ Reinforced strike plate
Window and Doors Briefing Notes: _____	

Characterize the construction of the weakest door that provides access to the facility or SAA
Blast resistant
A door that is designed, built and installed (to include the jamb or frame and hinges) to withstand some level of a blast. This would be a type of door that is obviously overbuilt and not a typical door at most facilities. Will normally not have a window. There should be some rating that indicates blast resistant.

Metal-clad
A metal clad door is typically a wood or fiberglass door that is enclosed in a thin sheet of sheet metal, aluminum, or steel. The door may appear to look like a typical solid front door to a home, but will have a rather tinny or metal sound when you knock on it with your hand. Should not have a window.

Hollow-steel
Very common commercial metal door. May or may not have a window. Generally made of light steel or aluminum. Will sound hollow when you knock on it with your hand.

Fire-rated door
Almost always made of steel or heavy gauge aluminum. Will normally have a sign attached that indicates the door must be closed at all times. Should not have a window, although some may have a small tempered wire encased glass window.

Wood, hollow core
Very typical interior commercial office door. Light, sounds hollow when you knock on it.

Wood, solid core
Typical interior office door. Slightly heavier than hollow door.

Metal or wooded framed glass (at least 50% of the door is glass)
Probably the most common door at most offices, buildings and arenas. This also applies to the rare door that is all glass and has no frame.

If present:
Interior or concealed hinges
Look for hinges that are on the interior of the building or built into the door jamb and prevent or hinder the ability to remove the door by removing the hinges.

Reinforced strike plate
This is often seen at high security facilities. It is normally a combination of a protected or shielded strike plate that inhibits the door from being opened by forcing the strike with a screwdriver combined with a metal or aluminum plate that surrounds the strike area and typically 3-6 inches of the door near the strike.

Building Envelope	
Wall	
Characterize weakest exterior/perimeter wall at the facility or SAA	☐ Poured Concrete ☐ Concrete masonry unit ☐ Brick ☐ Blast Panels ☐ Metal panels ☐ Stucco covered wood frame ☐ Wood frame ☐ Metal framed glass [all glass building]
Ceiling/Roof	
Characterize the weakest ceiling/roof for the facility or SAA	Are there skylights or openings that would allow entry (e.g., greater than 96 square inches)? ☐ No ☐ Yes If Yes, Are such openings protected with grates or other barriers? ☐ No ☐ Yes
Wall and Ceiling/Roof Briefing notes: _____	

Characterize weakest exterior/perimeter wall at the facility or SAA

Poured Concrete: Refers to any concrete structure that appears poured or framed verses concrete block. This also refers to prefabricated concrete that is typically built in as large slabs or some large shape of poured concrete. Many tall buildings and commercial facilities use poured or prefabricated concrete.

Concrete masonry units: Very simply, cement block. Typically 8" x 8" x 16" in size. Some refer to this as cinder block.

Brick: Come in various sizes, colors and shapes, but most common size in the U.S. is 8" x 4" x 2.5"

Blast Panels: Typically found in manufacturing facilities. May be found in museums, pharmaceutical companies, and chemical facilities, rarely in a hospital. Normally found in areas where some large quantity of flammable or explosive is used. Normally made of light sheet metal or fiberglass and are integrated seamlessly into the framework of a building. Typically can be identified by the type of fastening device to the framework, which will look different than other panels. Normally only located in one section of a facility or building near an area of explosives or highly volatile gases, liquids or solids. It is uncommon for an entire facility to be built with blast panels, but it is possible.

Metal panels
This and poured concrete are the most common building products for most of the facilities that receive SAV or IST visits. These range from sheet metal to fiberglass and are normally found on the exterior of a metal-framed building. They will be attached more securely and appear heavier and more durable than a blast panel.

Stucco covered wood frame
Unusual construction for commercial facilities. Typically found in the Western States. Normally used on smaller structures similar to a large home.

Wood frame
Unusual construction for most of the facilities that receive SAV or IST. Will typically be found on older construction and smaller facilities.

Metal framed glass [all glass building]
Modern and common material for tall buildings in urban areas.

Air Handling Systems	
Characterize the building air handling system for the facility or SAA	Does the facility/SAA have an air handling system? ☐ No ☐ Yes Does the system have outside air intakes? ☐ No ☐ Yes If yes, Location of the weakest external air intake to the facility or SAA (check only one): ☐ Greater than 30 feet above ground or roof mounted ☐ Greater than 10 feet but less than or equal to 30 feet (above ground level) ☐ From ground level to less than or equal to 10 feet or below grade (with restricted access to deter CBR contaminant) ☐ From ground level to less than or equal to 10 feet or below grade (with unrestricted access) Is the air handling controlled by a building control or SCADA system? ☐ No ☐ Yes If yes, ☐ Air handling can be controlled (shut off) by zones ☐ System has chemical/radiological/biological detection sensors ☐ System has chemical/radiological/biological effective filters ☐ System is able to provide both positive and negative pressure
Air Handling System Briefing Notes: _____	

Does the facility/SAA have an air handling system?
If it is an enclosed building, there is a good chance that there is an air handling system of some type. This definition or section does not typically want to identify a small window air conditioner. This is referring to the heating, ventilation and air conditioning system within a facility.

Does the system have outside air intakes?
It is unusual, though not impossible to have an HVAC system with internal intakes. The intent of this question is to identify the location of the intakes. The less accessible; the better.

Is the air handling controlled by a building control or SCADA system?
Most large facilities have some type of process control system that operates the HVAC. Rarely, the HVAC is attached to a SCADA system. Many of these large systems are designed that a third party (e.g. Johnson Controls) can monitor and control the system remotely.

If yes,
Air handling can be controlled (shut off) by zones
This allows various sections of the HVAC to be shut off in case of a dispersant. This also refers to reverse flow. In some cases a system is designed to exhaust and intake (very rare).

System has chemical/radiological/biological detection sensors
These are rare but can be found in some locations.

System has chemical/radiological/biological effective filters
These are rare but can be found in some locations. They are more common than sensors. Some filters have HEPA filters. Generally this section is looking for filters that go beyond HEPA, though many HEPA filters may be somewhat effective on some agents.

System is able to provide both positive and negative pressure
Another technique for isolating odors and contaminants is to design and operate the HVAC system so that pressure relationships between rooms are controlled. This control is accomplished by adjusting the air quantities that are supplied to and removed from each room. If more air is supplied to a room than is exhausted, the excess air leaks out of the space and the room is said to be under positive pressure. If less air is supplied than is exhausted, air is pulled into the space and the room is said to be under negative pressure. Control of pressure relationships is critically important in mixed use buildings or buildings with special use areas. Lobbies and buildings in general are often designed to operate under positive pressure to prevent or minimize the infiltration of unconditioned air, with its potential to cause drafts and introduce dust, dirt, and thermal discomfort. Without proper operation and maintenance, these pressure differences are not likely to remain as originally designed (see, Building Air Quality, A Guide for Building Owners and Facility Managers, Chapter 2 Factors Affecting Indoor Air Quality available at www.epa.gov/iaq/largebldgs/baq_page.htm.

Building Envelope	
Does facility/SAA have access ports to SAAs - other than a building (e.g.; hatches to bridge gear boxes, hatches to under bridge structural components, or secreted doors/hatches to outdoor concert stages)?	☐ No ☐ Yes If yes, the access port is protected/monitored by: ☐ Lock ☐ IDS ☐ CCTV ☐ Visual surveillance ☐ None *Describe:* _____
The facility/SAA sits above underground facilities not within the facility's control (e.g., utility tunnel, pedestrian tunnel, subway tunnel)	☐ No ☐ Yes If yes, facility or SAA can be accessed from the underground facility ☐ No ☐ Yes If yes, the access point is protected/monitored by: ☐ Lock ☐ IDS ☐ CCTV ☐ Visual surveillance ☐ None
Building Access Briefing Notes: _____	
Overall Building Envelope Comments: _____	

Does facility/SAA have access ports to SAAs - other than a building (e.g.; hatches to bridge gear boxes, hatches to under bridge structural components, or secreted doors/hatches to outdoor concert stages)? The intent here is to capture the access ports on a bridge, dam, or other structure that is not normally considered a building. This refers to maintenance hatches, access doors to catwalks or other areas that may be seldom used but are necessary for the routine or emergency maintenance and inspection of the structure. In some arenas there may be access hatches on stages that allow for stagehands or performers to enter during a performance and these may have limited access.

The facility/SAA sits above underground facilities not within the facility's control (e.g., utility tunnel, pedestrian tunnel, subway tunnel)

This section is trying to capture the unique access control areas that are typically out of control of the facility. Examples may be a subway or mass transit system that runs under a facility and has access to the facility in some manner. Pedways are another example. Also look for utility tunnels that may have openings or entrances to the facility.

Electronic Security Systems	
Exterior IDS	
Does the facility/SAA utilize an exterior intrusion detection system (IDS)? ☐ **No** ☐ **Yes** **If yes, characterize the exterior intrusion sensors *(check all that apply)***	Buried Line ☐ Fiber-optic cable ☐ Seismic pressure ☐ Magnetic field ☐ Ported coaxial cable ☐ None Fence Associated ☐ Electric Field ☐ Sensor Fence ☐ Fence disturbance (taut wire) ☐ None Free-Standing ☐ Active infrared ☐ Passive infrared ☐ Bistatic microwave ☐ Video motion detection ☐ None
Exterior IDS monitoring and assessment by facility:	Characterize the facility's monitoring of the external IDS: ☐ Continuously monitored: onsite ☐ Continuously monitored: offsite ☐ Interface Software (if activated) ☐ Backup power provided ☐ Tamper and system problem indicators provided ☐ Positioned to prevent gaps in coverage ☐ Detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris) ☐ Compensatory measures employed when alarms are not Operating ☐ Linked to Emergency Services ☐ None *Describe*: _____ Characterize the facility's assessment of exterior IDS alarms: ☐ Not assessed by facility ☐ Assessed *If assessed, check all that apply:* ☐ Notifies local response agencies ☐ Automatic Deployment of Security Force ☐ CCTV ☐ Deployment of employee/personnel other than security force *Describe*: _____

ELECTRONIC SECURITY SYSTEMS

INTRUSTION DETECTION SYSTEMS (IDS)

All IDS questions apply only to the primary facility or facilities that house significant assets or areas (SAAs). Do not answer questions on the types of IDS in buildings that do not house SAAs. Exterior sensors are used in an outdoor environment (e.g., fence, exterior windows or exterior doors) and interior sensors are those used inside buildings (e.g., doors into a critical IT server room). It is possible to have a local door or window alarm that is not part of an IDS and there is no need to answer the questions in this section if that is the case. If the facility is not within a building, do not answer the questions for internal IDS.

Does the facility utilize an external detection system?

Seismic pressure – Passive, covert terrain-following sensors that are buried in the ground. They respond to disturbances of the soil caused by an intruder walking, running, jumping, or crawling on the ground.
Magnetic field – Passive, covert, terrain-following sensors that are buried in the ground. They respond to a change in the local magnetic field caused by the movement of nearby ferromagnetic material. It is effective at detecting vehicles or intruders with weapons.
Ported coaxial cable – Active, covert, terrain-following sensors that are buried in the ground. They are also known as leaky coax or radiating cable sensors.
Fiber-optic cable – Optical fibers are long, hair-like strands of transparent glass or plastic. A single strand of fiber-optic cable, buried in the ground at the depth of a few centimeters, can very effectively give an alarm when an intruder steps on the ground above the fiber.

Fence Associated
Fence Disturbance – passive, visible, terrain-following sensors that are designed to be installed on a security fence, typically constructed with chain-link mesh.
Sensor Fence – Passive, visible, terrain-following sensors that make use of the transducer elements to form a fence itself.
Electric Field (also known as Capacitance) are active, visible, terrain-following sensors that are designed to detect a change in capacitive coupling among a set of wires attached to, but electrically isolated from, a fence.

Free Standing
Active Infrared – A sensor that detects the loss of the received infrared energy when an opaque object blocks the beam.
Passive Infrared – A sensor that detects the presence of human thermal energy emissions and causes an alarm to be generated.
Bistatic microwave – Active, visible, line-of-sight, freestanding sensors. Two microwave antennas are installed on opposite ends. One is connected to a microwave transmitter, the other to a microwave receiver that detects the received microwave energy. Usually installed to detect a human crawling or rolling on the ground across the microwave beam, keeping the body parallel to the beam.
Dual technology – The concept is to place both a passive infrared and a monostatic microwave in the same housing. The theory is that the sensors will not alarm until both have been activated, thus avoiding nuisance alarms.
Video motion detection – Passive, covert, line-of-sight sensors that process the video signal from closed-circuit television cameras. They sense a change in the video signal level for some defined portion of the viewed scene.

Electronic Security Systems	
	Characterize the external IDS alarm enunciators: ☐ Ultrasonic sound alarm ☐ Multiple linked technologies (e.g., Sonitrol Technology) ☐ Audible Remote ☐ Visual Remote ☐ Visual Local ☐ Audible Local ☐ Silent ☐ None Is the exterior IDS maintained according to recommended specifications? ☐ Unknown ☐ No ☐ Yes Is the exterior IDS tested periodically? ☐ Unknown ☐ No ☐ Yes
Exterior IDS Briefing Notes: _____	

Characterize the intrusion alarm enunciators

Audible Local is where the alarm simply sounds audibly at the area affected by the alarm.

Audible Remote is where the alarm sounds audibly at a panel in a command center or security area not located at the area affected by the alarm.

Visual Local is a flashing light or other visual indicator that the alarm has been triggered, but can only be seen from at the area affected by the alarm.

Visual Remote is a flashing light or other visual indicator that the alarm has been triggered, but can be seen at a panel in a command center or security area not located at the area affected by the alarm.

Ultrasonic sound alarm is where a detection field is established using energy in the acoustic spectrum and detection is based on the frequency shift between the transmitted and received signals caused by the Doppler effect from a moving object in the beam.

Multiple Linked Technology is when the IDS alarm enunciator is tied other technologies such as verified audio detection, digital video surveillance, access control systems, and even fire detection (e.g., Sonitrol or motion alarmed cameras).

Silent is where the alarm does not sound at the area affected by the alarm, but results in some indicator (e.g., sound or visual) at a remote location.

None is where there are no alarm enunciators.

Intrusion Alarm Assessment: System maintained according to recommended specifications
Mark unknown if facility personnel do not know. (Although, if the appropriate personnel do not know if the system is maintained; it probably is not.)

Is the external IDS tested periodically?
Testing could include running the IDS system on the backup generator, checking that alarms correctly work when the sensor is activated, or other methods of ensuring the IDS work properly and are viewing and recording as required.

Electronic Security Systems	
Interior IDS	
Does the facility/SAA utilize an interior intrusion detection system? ☐ **No** ☐ **Yes** **Characterize the interior motion sensors. *(check all that apply)***	Boundary Penetration Sensors ☐ Fiber Optic Cable ☐ Capacitance ☐ Infrared ☐ Electromechanical ☐ Vibration ☐ Photoelectric ☐ None Interior Motion Sensors ☐ Ultrasonic noise detection ☐ Microwave ☐ Sonic ☐ Passive Infrared ☐ None Proximity sensors ☐ Capacitance ☐ Pressure ☐ None Door Sensors ☐ Glass Breakage Sensor ☐ Grid Mesh ☐ Vibration Sensor ☐ Balanced magnetic contacts ☐ Conducting tape ☐ None Window Sensors ☐ Glass Breakage Sensor ☐ Grid Mesh ☐ Vibration Sensor ☐ Magnetic contact ☐ Conducting Tape ☐ None

Does the facility utilize an interior detection system?

Boundary Penetration Sensors
Electromechanical – Passive, visible, line sensors. The most common type is a relatively simple switch generally used on doors and windows. Most switches are magnetic.

Infrared – Visible line sensors. These sensors establish a beam of infrared light using an infrared light source as the transmitters and photo detectors for receivers.

Vibration – Passive sensors that can be visible or covert. They detect the movement of the surface to which they are fastened. They may be as simple as jiggle switches or as complex as internal switches or piezoelectric sensors.

Capacitance – They establish a resonant electrical circuit between a protected metal object and a control unit, making them active sensors.

Fiber Optic Cable - Passive line detectors that can be visible or covert. Optical fibers are long, hair-like strands of transparent glass or plastic. A single strand of fiber-optic cable, buried in the ground at the depth of a few centimeters, can very effectively give an alarm when an intruder steps on the ground above the fiber.

Interior Motion Sensors
Microwave – Active, visible, and volumetric sensors. They establish an energy field using energy in the electromagnetic spectrum, usually at frequencies on the order of 10GHz. They can be used in monostatic operation.

Ultrasonic noise detection – Active, visible, volumetric sensors. They establish a detection field using energy in the acoustic spectrum typically in the frequency range between 19 and 40 kHz. They can be used in monostatic operation.

Sonic - Active, visible, and volumetric sensors. They establish a detection field using energy in the acoustic spectrum at frequencies between 500 and 1000 Hz. They can be used in monostatic, bistatic, or multistatic modes of operation.

Passive Infrared - A sensor that does not transmit a signal for an intruder and senses the radiation from a human body.

Proximity sensors
Capacitance – Active, covert line sensors. They can detect anyone either approaching or touching metal items or containers that the sensors are protecting. They establish a resonant electrical circuit between a protected metal object and a control unit.

Pressure – Often in the form of mats, placed around or underneath an object. They are passive, covert, line detectors. Constructed so that when an adequate amount of pressure, depending on the application, is exerted anywhere along the ribbon, the metal strips make electrical contact and initiate an alarm.

Door Sensors
Vibration sensors detect the movement of the door.

Glass Breakage Sensor, mounted directly on the glass, are vibration sensors designed to generate an alarm when the frequencies more nearly associated with breaking glass are present.

Conducting Tape is typically some type of copper tape that carries a weak signal to a sensor of some type. When the contact of the tape is broken, the signal is broken and the sensor sets off some type of alarm

This page is intentionally left blank

Grid Mesh is a type of vibration sensor that uses mesh within a window that both prevents glass from shattering as well as sets off the alarm.

Magnetic contact is similar to conducting tape. In this case the magnetic field is the sensor and when that field is interrupted an alarm of some type is activated.

Window Sensors
Vibration sensors detect the movement of the window.

Glass Breakage Sensor, mounted directly on the glass, are vibration sensors designed to generate an alarm when the frequencies more nearly associated with breaking glass are present.

Conducting Tape is typically some type of copper tape that carries a weak signal to a sensor of some type. When the contact of the tape is broken, the signal is broken and the sensor sets off some type of alarm.

Grid Mesh is a type of vibration sensor that uses mesh within a window that both prevents glass from shattering as well as sets off the alarm.

Magnetic contact is similar to conducting tape. In this case the magnetic field is the sensor and when that field is interrupted an alarm of some type is activated.

Electronic Security Systems	
Interior IDS monitoring and assessment by facility:	Characterize the facility's monitoring of the interior IDS ☐ Continuously monitored: onsite ☐ Continuously monitored: offsite ☐ Interface Software (if activated) ☐ Backup power provided ☐ Tamper and system problem indicators provided ☐ Positioned to prevent gaps in coverage ☐ Detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris) ☐ Compensatory measures employed when alarms are not operating ☐ Linked to Emergency Services ☐ None Characterize the facility's assessment of interior IDS alarms. ☐ Not assessed by facility ☐ Assessed *If assessed, check all that apply:* ☐ Notifies local response agencies ☐ Automatic Deployment of Security Force ☐ Automatic deployment of employee/personnel other than security force ☐ CCTV Characterize the interior IDS alarm enunciators: ☐ Ultrasonic sound alarm ☐ Multiple linked technologies (e.g., Sonitrol Technology) ☐ Visual Remote ☐ Audible Remote ☐ Visual Local ☐ Audible Local ☐ Silent ☐ None Interior IDS is maintained according to recommended specifications ☐ Unknown ☐ No ☐ Yes
Interior IDS is tested periodically	☐ Unknown ☐ No ☐ Yes
Interior IDS Briefing Notes: _____	

Characterize the facility's monitoring of the interior IDS
Continuously monitored: onsite is where the alarm panel is monitored at an onsite security command center or area.

Continuously monitored: offsite is where the alarm panel is monitored at an offsite contract or centralized company security command center or area.

Positioned to prevent gaps in coverage is to ensure that the sensors are placed to spaces that are not covered by the IDS.

Characterize the facility's assessment of interior IDS alarms.
Not assessed by facility means facility personnel do not conduct an assessment or evaluate why the alarm was activated. If there is an assessment when the alarm is activated, characterize that assessment.

If assessed,
Notifies local response agencies is when the alarm is monitored at the local police department or fire department.

Automatic Deployment of Security Force is when the alarm results in security personnel making a physical visit to the area affected by the alarm.

Automatic deployment of employee/personnel other than security force is when the alarm results in personnel other than security personnel are deployed such as receptionist, desk clerk, operations personnel.

CCTV is that personnel consult the appropriate CCTV console to view the area affected by the alarm.

Characterize the interior IDS alarm enunciators:
Audible Local is where the alarm simply sounds audibly at the area affected by the alarm.

Audible Remote is where the alarm sounds audibly at a panel in a command center or security area not located at the area affected by the alarm.

Visual Local is a flashing light or other visual indicator that the alarm has been triggered, but can only be seen from at the area affected by the alarm.

Visual Remote is a flashing light or other visual indicator that the alarm has been triggered, but can be seen at a panel in a command center or security area not located at the area affected by the alarm.

Ultrasonic sound alarm is where a detection field is established using energy in the acoustic spectrum and detection is based on the frequency shift between the transmitted and received signals caused by the Doppler effect from a moving object in the beam.

Multiple Linked Technology is when the IDS alarm enunciator is tied other technologies such as verified audio detection, digital video surveillance, access control systems, and even fire detection (e.g., Sonitrol or motion alarmed cameras).

Silent is where the alarm does not sound at the area affected by the alarm, but results in some indicator (e.g., sound or visual) at a remote location.

None is where there are no alarm enunciators.

This page is intentionally left blank

Intrusion Alarm Assessment: System maintained according to recommended specifications
Mark unknown if facility personnel do not know. (Although, if the appropriate personnel do not know if the system is maintained; it probably is not.)

Is IDS tested periodically?
Testing could include running the IDS system on the backup generator, checking that alarms correctly work when the sensor is activated, or other methods of ensuring the IDS work properly and are viewing and recording as required

<table>
<tr><th colspan="4">Electronic Security Systems</th></tr>
<tr><th colspan="4">Closed Circuit Television (CCTV)</th></tr>
<tr><td>Does the facility utilize CCTV?</td><td colspan="3">☐ No (Go to next section)</td></tr>
<tr><td></td><td>☐ Yes</td><td colspan="2">(% of area covered)
(0, 1-25%, 26-50%, 51-75% or 76-100%)

☐ Perimeter _____%
☐ Area of concern (e.g., gate, entry way) _____%
☐ Critical areas/SAA (e.g., control stations) _____%</td></tr>
<tr><td>Characterize the technology.</td><td colspan="2"><u>Type</u>
☐ Digital
☐ Analog

<u>Capability</u>

☐ Image intensification (low-light)
☐ Infrared
☐ Color
☐ Black & White

<u>Functionality</u>
☐ Pan-Tilt-Zoom
☐ Panoramic Lens or software
☐ Fixed</td><td><u>Transmission Media</u>
☐ Fiber cable
☐ Wire line (twisted pair)
☐ Coaxial
☐ Telephone wire
☐ Wireless

<u>Emergency Backup Power</u>
☐ No
☐ Yes

<u>Video analytics or Anomaly Detection</u>
☐ No
☐ Yes</td></tr>
</table>

CLOSED CIRCUIT TELEVISION (CCTV)

Does the facility utilize CCTV? For percentage of coverage, select either: 0, 1-25%, 26-50%, 51-75% and 76-100% for each area covered. If 0 is selected, it means that no part of this area is covered.

Characterize the technology.

Type

Digital Almost all systems put in place within the last 5 years are likely digital. This refers to the record and display system along with the cameras. If there is a DVR, there is a really good chance the system is digital.

Analog This is almost always an older system. This refers to the record and display system along with the cameras. If the record system is VCR tape, the system is analog.

Capability

Image intensification (low-light) (sometimes called "Day/Night Cameras") are regular cameras with a highly sensitive CCD chip with the ability to capture quality imagery with very little light present.

Infrared is an illuminator camera creates light in no-light situations.

Functionality

Pan-Tilt-Zoom cameras allow you to adjust the position ('pan' is side-to-side, 'tilt' is up-and-down) and focus ('zoom') of the camera using a remote controller.

Panoramic Lens or software allows cameras to see a wider-range of view (360°) without moving.

Fixed cameras have a straight view that does not change.

Transmission Media

Fiber Cable is a cable made up of super-thin filaments of glass or other transparent materials that can carry beams of light.

Wire line (twisted pair) is a cable with multiple pairs of twisted insulated copper conductors in a single sheath.

Coaxial is a cable transmission, which may be base-band video or video-modulated radio frequency.

Wireless is either a microwave or IP network to send information with sufficient bandwidth.

Video analytics or Anomaly Detection

Video analytics refers to any software program that aids in eth determination of suspicious activity. This can be through dwell time, package recognition or any other process where some type of software adds to the process. Anomaly detection is where a video motion processor establishes localized features in the live image that are distinct enough to be tracked from frame to frame. The system builds up a statistical history of how such features normally move through the image, tracking their speed and direction. Then when the CCTV image changes, the system can check against what it has established as normal to decide whether the new event is so unusual that it should be brought to an operator's attention.

Electronic Security Systems	
Who monitors the CCTV cameras	☐ Dedicated, 24/7 trained security staff For dedicated, 24/7 staff: ☐ CCTV monitoring shift rotates at least every hour ☐ No more than 16 cameras are monitored by each staff member ☐ None of the above ☐ Trained, but not dedicated, security staff ☐ Non-security personnel (e.g., receptionist) ☐ No real-time monitoring (only review recorded information) ☐ Law enforcement monitoring in addition to facility staff
Is the CCTV recorded?	☐ No ☐ Yes If yes, mode of recording: ☐ Digital ☐ Analog If yes, is there a policy for review of recorded information ☐ No ☐ Yes If yes, is review ☐ Periodic ☐ Only after an incident
How long is the recorded information stored?	☐ More than a month ☐ More than a week to a month ☐ More than 72 hours to a week ☐ 24 – 72 hours ☐ Less than 24 hours ☐ Not stored

Who monitors the CCTV cameras?
Can check more than one, as applicable. If the staff is dedicated 24/7/365 with sole purpose to watch, monitor and coordinate response and is also trained to recognize potential indicators, etc., check both. If the CCTV is monitored by an untrained receptionist or administrative person as a casual assignment, do not check either trained or dedicated; there it is assumed to be no CCTV monitoring. **If none of the selections are chosen, it will be assumed there is no monitoring of the CCTV camera system.**

Dedicated Staff is defined as 24/7/365 staff that has the sole purpose to watch, monitor and coordinate response to activity on video. The individuals are trained on surveillance detection.
Trained Staff is defined as less than 24/7/365 coverage, trained in potential indicators; however have other duties in addition to watching CCTV display.
Non-security personnel (e.g., receptionist) is anyone other than dedicated staff or trained staff.
No real-time monitoring (only review recorded information) is when no one is monitoring the CCTV
Law Enforcement monitoring in addition is defined as an outside public agency monitoring the facility via camera. This could include:

- DHS Webcam
- Live feed to 911 center
- Direct Feed to Police Station

This would not include public camera systems where the facility just happens to be within the coverage of cameras for monitoring stoplights or speeding.

Electronic Security Systems	
Closed Circuit Television (CCTV)	
Is CCTV system maintained according to recommended specifications?	☐ Unknown ☐ No ☐ Yes If Yes, ☐ Maintenance or repair done by "in-house" personnel ☐ Maintenance or repair done by contracted personnel
Most recent update to CCTV system	☐ Within 1 year ☐ 1-3 years ☐ 3-5 years ☐ More than 5 years
Is the CCTV system tested periodically?	☐ Unknown ☐ No ☐ Yes
CCTV Briefing Notes: _____	
Overall CCTV Comments: _____	

Is CCTV system maintained according to recommended specifications?
Maintenance should be in accordance with industry practice or equipment manufacturer recommendations. In addition, the maintenance or repair may be done by "in-house" personnel (e.g., employee IT teams) or by contracted personnel (e.g., a contract with the manufacturer for maintenance/repair or with an outside contractor that provides service on this type of equipment).

Is the CCTV system tested periodically?
Testing could include running the CCTV system on the backup generator, checking camera vies by using well-placed vehicles or people to ensure the camera is properly aligned with the focus area, or other methods of ensuring the cameras work properly and are viewing and recording as required.

Illumination			
	Fences, Gates, Parking areas	**Building entrance and delivery areas**	**Waterside Facilities**
Not applicable: Illumination does not apply since facility or SAA does not include these areas (for areas selected do not answer any other Illumination questions)			
Not Illuminated: Area is not illuminated in any manner, but reasonably should be illuminated. (there is no illumination installed specifically designed to cover this area)			
Not Illuminated On Purpose: Facility has made a security decision to not illuminate this area; Illuminating the area increases the vulnerability.			
Illumination Type and Operation Briefing Notes: _____			

ILLUMINATION

General information: Illumination is broken into areas that likely would have similar illumination. When looking at fences, gates and parking areas, consider all exterior areas on the perimeter of the facility or exterior of the buildings or SAA's. It is expected that not all facilities will have each of the specific items of fence, gate and parking. If a facility does not have a fence and gate but has parking, select the responses based on parking alone. For building entrance and delivery areas the concept is to look at the exterior areas. It is expected that not all facilities will have a delivery dock. It may be that the entrance and delivery area is the same. Waterside facilities is not applicable unless the facility is along or on the water. The water may be a lake, river, ocean or similar type of body of water. It generally does not include retention ponds or some type of drainage ditch. Facilities that typically fall into this category are locks, dams, power plants, water treat, wastewater treatment, fertilizer or chemical manufacturing, refineries, and marinas. *Regardless of the area being evaluated, the focus should be on the weakest or most vulnerable area.*

Not Applicable: If a facility does not have any fences, gates or parking then not applicable should be selected. The most common selection for not applicable will be waterside facilities. Once not applicable is selected, no other selections are required in that column.

Not Illuminated: This selection would apply if there is no illumination covering one of the areas, but you as a professional security person would expect the area to have some illumination. For example, it would be unusual to have a parking lot in a mall without some illumination. If you have gates, fences and parking at a given facility and parking and gates are illuminated, but the fence is not and the fence logically should be illuminated, then the best answer is "Not Illuminated" in the fences, gates and parking areas column. If you have multiple gates but only some of the gates are illuminated, then you as a security professional must determine if the non-illuminated gates are significant enough to operations that they should be illuminated. If the gate leads to a corporate ball diamond, it would probably not be significant. If the gate leads to the facility and once inside a person has access to the entire facility operations, it is likely significant enough to include the illumination factor. Once not illuminated is selected, no other selections are required in that column.

Not Illuminated On Purpose: This will be used rarely, but is possible. In some cases a facility has determined that illuminating an area showcases or highlights a vulnerability. This is more likely at a particular SAA verses an entire facility. There may be lights at a given SAA or facility, but the owner operator has made a conscious and reasoned decision to not turn the lights on or disabled them for the explicit purpose of increasing security. This is sometimes referred to as security through obscurity. Some facilities that may use this type of security include dams, chemical plants, manufacturing facilities and telecomm hotels. This selection should be used sparingly and only applies in isolated cases. Once not illuminated on purpose is selected, no other selections are required in that column.

Illumination			
	Fences, Gates, Parking areas	**Building entrance and delivery areas**	**Waterside Facilities**
Uniformity			
Illumination appears to be similar and uniform in type with overlapping light pattern coverage in most areas			
Illumination appears to be of different types causing shadows or glare, however there is an overlapping light pattern coverage in most areas			
Illumination appears to be similar and c onsistent in type, however light pattern coverage does not overlap causing shadows or dark areas			
Illumination appears to be uneven and dissimilar in type causing glare and shadows with inconsistent coverage in most areas creating dark areas and shadows			
Illumination Type and Operation Briefing Notes: _____			

Uniformity: Uniformity refers to a combination of type and coverage. It is understood that most visits will be in the daytime and lights may not be illuminated. While the best situation is that a visit also occurs at night or a drive by of the facility at night occurs, it is also understood that this is often not practical or even reasonable.
An approximate determination of uniformity can be made by looking at the type of light and the spacing of the light fixtures.

Similar and uniform in type
Type of illumination takes into consideration the type of bulb or light emitted. Look for similar type bulbs whether that is incandescent, halogen, low-pressure sodium, LED or one of the many other types. If the bulbs appear similar, it can be assumed that illumination is uniform. If you see several different types of bulbs, then it is unlikely to be uniform. Concerning coverage, obviously in the daytime this is a challenge. One approximation can be made by looking at the spacing of the fixtures, the height and locations of the fixtures, items that might block light or create shadows, and then combine that information with the type of illumination to make an approximation.

Overlapping light pattern coverage
Uniform and overlapping illumination would indicate that lights are of the same type bulb, fixtures are spaced to allow overlap without creating significant shadows, and blocked areas are illuminated by the same type of bulb and sufficient fixtures. Overlapping coverage with different types of lights will create shadows or glare.
Similar type illumination that does not overlap allows for shadows and dark areas. Dissimilar illumination with inconsistent coverage creates glare, shadows, and dark areas and would be unacceptable by most security professional.

Illumination			
	Fences, Gates, Parking areas	**Building entrance and delivery areas**	**Waterside Facilities**
Operation			
Illumination is constant. Is turned on m anually and / or automatically through photo cell or time switch and stays on during hours of darkness or is on all the time.			
Illumination is triggered by motion detectors or is part of an alarm system.			
Lights appear to be in good repair in most areas, and there are no burned out bulbs in critical locations.			
Lights appear to be in need of repair or maintenance in most areas, however there are no burned out bulbs in critical locations.			
Lights appear to be in good repair in most areas, however, there are burned out bulbs in critical locations.			
Illumination Type and Operation Briefing Notes: _____			

Operation: Operation incorporates the basic function of the lights and addresses the maintenance.

Constant illumination is turned on manually or by photo cell or some type of timing device. It is expected that this type of illumination is either on during all hours of darkness or is on all the time. It is normal for some bulbs to intermittently shut off and recover as part of their normal process. That is understood and should not be considered intermittent illumination. It is expected that many facilities would be able to select constant illumination.

Illumination triggered by motion detectors or as part of an alarm system generally add to security by illuminating areas as needed when triggered.

Maintenance of lights is obviously best determined at night, but that is not always practical or reasonable. A reasonable approximation can be made by looking at the condition of the luminaries. If the luminaries appear to be in good repair and there does not appear to be any burned out bulbs in critical locations that is generally considered positive. In some cases luminaries may appear in need of repair but there are no burned or broken bulbs. That is not the best situation, but the area is illuminated. Finally if broken or burned out bulbs are identified, that may become an option for consideration.

Illumination			
	Fences, Gates, Parking areas	**Building entrance and delivery areas**	**Waterside Facilities**
Backup power			
Illumination backup power supply covers most of existing lights and critical locations			
Illumination backup power supply does not cover most of existing lights, however it does cover critical locations			
Illumination backup power supply covers emergency lighting, however it does not cover most critical locations			
Illumination has no backup power supply, or does not provide coverage to critical locations.			
Special Situations			
Portable lighting available onsite for emergencies or heightened threat levels			
Searchlights or high intensity lights in use			
Illumination Backup Power and Special Situations Briefing Notes: _____			
Overall Illumination Section Comments: _____			

Backup: Backup power should be answered specific to illumination; however, this does not mean that illumination requires a separate and unique generator or UPS. It is sufficient if the facility or SAA backup power supply includes illumination. Of course, if for some reason the illumination has its own backup generator that is fine, but not required. In the best case, most if not all of existing luminaries have some type of backup power. This may be an UPS or generator. Most important is that illumination in critical areas is covered. The other selections available range from not covering critical areas, covers only emergency lighting (escape or exit lights) to not having any backup coverage at all.

Special Situations: These items are found in select areas and are typically not found at all facilities. Portable lighting is defined as generator or battery driven high intensity light, much like is seen on highway road construction. The idea is to have this additional illumination available for emergencies or increased threat levels. Searchlights or high intensity lights are most commonly seen at waterside facilities. Typically this refers to lights on docks used for illumination of loading and unloading ships. This type of additional lighting is normally portable, but may be at a fixed location (e.g., prison turret). It is used in addition to normal illumination in the area to enhance visibility or illumination of a significant asset or feature of a facility.

DEPENDENCIES

Dependencies are a fundamental consideration when assessing the resilience of critical infrastructure assets and, ultimately, the resilience of a region. Critical infrastructure assets support the functioning of a region by providing essential resources used by other critical infrastructure, government entities, or the population. Dependencies are the linkages between two critical infrastructure assets, through which the state of one infrastructure influences or is correlated to the state of the other. It is important to thoroughly characterize dependencies when seeking to reduce the extent to which the facility is directly affected by the missions, functions, and operations of other critical infrastructure assets.

The general concept for addressing each critical resource is to determine the use for the resource, whether there are redundant services (e.g., internal production or alternative fuels), what protections are in place to maintain service (e.g., the electric transformers at a facility are protected by fencing, locked gates, privacy slats and crash bars) and backup (e.g., emergency generator or UPS). Lastly, the criticality of the resource is determined by estimating the time it will take for the facility to experience a severe impact once primary service is lost, what percentage of facility operations can be maintained with and without backup service in place (e.g., a backup electric generator may only provide power to run a plant at 50 percent production) and if any external regulations/policies are in place that require shut down of the facility due to service disruption of a critical resource (e.g., a fire code that requires evacuation of a building if water service is lost or production/operations specifications for a constant temperature for chemical manufacturing).

Information collected with these questions directly addresses an important element of the following PS-Prep standards:

NFPA1600: "Operational impact, including upstream and downstream operations and dependencies or cascading impact, or both, both internal and external to the entity". "Global dependencies, which are the dependencies between an organization's multiple facilities and external entities and are assessed to determine the propagation of interruptions."

ASIS SPC.1-2009: "Consider its dependencies on others and others dependencies on the organization, including critical infrastructure and supply chain dependencies and obligations"

The term "dependency," as used in the IST, is defined as the reliance of a facility on a specific resource to carry out its "core operations."

Does the facility use this resource for its Core Operations?

Core Operations include any critical function that is necessary for the facility to fulfill its mission. For instance, clearly natural gas used for process operations is a core function. Natural gas used for cooking in the executive cafeteria is not a core function; however, natural gas used for cooking at a restaurant would be a core function. Natural gas used for cooking at a hospital could support a core function (i.e., providing food to patients – but not to the visitor cafeteria)

Answer the following sections **only if "Yes" is selected**. The questions **focus on the primary external source**, but will also address the capacity of any secondary internal sources. If for a given resource (e.g., electric power, natural gas, communications, etc.), the facility **is not dependent on an external supplier**, the facility, it is considered that **the facility is not dependent on the resource**.

Note:
As an example a water treatment plant often uses electric power, supplied by an external provider, for equipment and normal office functions, communications for dispatching repair crews, IT service for process controls, and critical chemicals such as chlorine. However, even if it needs raw water (obviously the facility has no treatment function without the raw water), this raw water is not provided by an outside organization, unless the facility is buying the water from an outside source and in that the case, it would be a critical product/raw material. In conclusion, a water treatment plant does not use wastewater. Similarly, a wastewater treatment plant is not dependent on the incoming wastewater nor is an electric substation dependent on the electricity running through it as part of the grid; that is the facility's function. However, if the substation has a control house or electric switches, it will need what is often referred to as "station power" from an external source (usually a drop line from the local distribution grid).

Dependencies – Electric Power	
Electric Power	Is external electric power required for Facility core operations (e.g., produce key services/goods)? ☐No ☐Yes If yes, complete this section. Primary use for Electric Power: *(Check all that apply)* ☐ On-site heat / hot water ☐ Core Operations (including lighting, IT, telecom, etc.) ☐ Security Operations (e.g., CCTV, scanners, sensors, etc.) *Describe:* _____
External Sources	Is the external source the primary source? ☐ No ☐ Yes What is the name of the Provider/Supplier: _____ **Provider Facilities serving the facility:** Provider/supplier substation(s) servicing facility: ☐ Unknown Name or location: _____ Describe: _____ (if multiple substations) Name or location (2nd substation): _____

DEPENDENCIES – ELECTRIC POWER

For Electric Power, the question set captures both external and internal sources of power. However, if **the facility does not receive any electric power from an external source** (all electric power is generated internally), please **check NO below and go to the next section: Dependencies – Natural Gas**

If part or all the electric power needed for the facility core operations originates from an external provider, please provide the information requested in this section.

Is the external source the primary source?

Answer to this question is **yes** if at least 51% of the electric power needed for the facility core operations is provided by an external source.

Dependencies – Electric Power	
External Sources	**Entrances to Facility:** How many electric service connections are there for the facility? ☐ One service connection ☐ More than one service connections If more than one, can each service connection handle entire facility load? ☐ No ☐ Yes *Describe*: _____ If there are multiple service connections, where do the lines enter the facility? ☐ Same location ☐ Different geographic locations *Describe*: _____ Service connections into the facility are located ☐ Aboveground (power poles) ☐ Buried ☐ Mixed (both aboveground and buried) Are the service connections co-located with other utilities (e.g., utility corridors for natural gas, communications, fiber, water)? ☐ No ☐ Yes *Describe*: _____ Are there protective measures in place inside the building supporting the electrical system (e.g., locked electrical cabinet or room)? ☐ No ☐ Yes *Describe*: _____ Are there protective measures in place outside the building supporting the electrical system (but still within control of facility, e.g., bollards or box around facility-owned transformer)? ☐ No ☐ Yes *Describe*: _____
Electric Power External Sources Briefing Notes: _____	

Service Connections into the facility are located
To determine the location of service connections, consider everything between where the service enters the facility's property line until it terminates at the facility's system (e.g., the meter in the basement or the electric box outside the barn).

Are there protective Measures in place inside the facility supporting the electrical system
This question ascertains if the supporting electric components are protected from accidental or purposeful damage. For example, if the electric transformers for the facility are within the facility line but are located in the parking lot (without protection) where trucks can back into them, the answer would be NO. Conversely, if facility step-down transformers are located outside the facility fencing (but on the facility property within the facility's control), and have adequate fencing, locked gates, privacy slats and crash bars so the answer would be YES. Buried service lines are considered protected, so the answer would be YES.

Dependencies – Electric Power	
Internal Sources	Does the facility have an internal electric power source? ☐ No ☐ Yes If yes, is the internal source the primary source? ☐ No ☐ Yes Internal power provided by (select one) ☐ Power Plant onsite ☐ Cogeneration unit onsite Which fuel(s) are used by the Power Plant/Cogeneration Unit: ☐ Natural Gas ☐ Petroleum ☐ Other Does Power Plant/Cogeneration unit generate enough electricity to handle full facility load? ☐ Yes ☐ No If no, estimate the percent of peak facility demand the plant can supply: _____%
Electric Power Internal Source Briefing Notes: _____	

Is the internal source the primary source?
Answer to this question is **yes** if at least 51% of the electric power needed for the facility core operations is generated internally by the facility.

Cogeneration unit onsite
Cogeneration is a generating facility that sequentially produces electricity and another form of useful thermal energy (such as heat or steam or useful mechanical work such as shaft power) used for industrial, commercial, residential or institutional purposes.

These questions inform us whether a co-generation unit is an adequate backup or redundant electric source. An example of an inadequate backup is when plant processes requiring electricity stop when electric power is lost and the bottoming cycle unit cannot make electricity because it requires the fuel generated by the plant processes' byproduct (e.g., a generation plant that uses byproduct/waste methane generated as part of a process as its fuel to make electricity). Conversely, if the cogeneration unit is fueled directly by an outside source of natural gas and the external electricity source is lost, the cogeneration unit will be able to function.

Dependencies – Electric Power	
Electric Power Loss of External Source	Has the facility experienced electric service outages within the last year? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If external electric service is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external electric service is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after total loss of electric service including backup? ☐ No ☐ Yes *Describe*: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) *Describe*: _____
Electric Power Loss of External Source Briefing Notes: _____	

Is there a contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of electric power.

Does the facility participate in provider priority plan for restoration
A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If external electric service is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)?

This question captures the impact of the worst case scenario: the fact that the facility loses electric power and is unable to operate its backup.

Once electric service is lost (without considering any backup or alternative mode)
This question captures the impact of the worst case scenario: the fact that the facility loses electric power and is unable to operate its backup.

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down if facilities functions are degraded after loss of the main source of electric power. The answer is YES if the facility has specific procedures defining that the facility must shut down due to loss of electric power. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of electric power) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the external electric power supply is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements or preparations for re-energizing sensitive equipment (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external sources of electric power. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of electric power is lost during 7 days, what time will be needed for full resumption of core operations when the external sources of electric power is restored.

Dependencies – Electric Power	
Alternates and Backup Generation	**Does the facility have an alternate or backup that can be used in case of loss of external source?** ☐ No ☐ Yes If yes, please provide the following information Once external electric service is lost (**and considering your backup or alternative**), what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% **Does the facility have a Backup generator?** ☐ No ☐ Yes Type of backup generator (diesel generator, natural gas) ☐ Diesel Generator ☐ Natural Gas (pipeline) ☐ Propane ☐ Other Is refueling necessary ☐ No ☐ Yes If yes, Fuel Supplier Name: _____ ☐ Contracts or procedure in place for refuel in emergency Duration of backup generation without refueling _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Purpose of the backup generator (check one): ☐ Life Safety ☐ Graceful shutdown ☐ Core Operations ☐ Entire Facility Load

Alternates and Backup Generation
The intent of this section is to capture alternates and backups (backup generator and U ninterrupted Power System) in place in the facility that can provide electric power in case of loss of the external source of electric power.

Once external electric service is lost (and considering your backup or alternative mode)
This question captures the facility capability to operate in case of disruption in the external supply of electric power. This information should take into account UPS batteries, backup generators, internal sources or any other alternatives at the disposal of the facility for supplying electric power in case of failure of the primary external source.

Dependencies – Electric Power	
Alternates and Backup Generation	Is backup routinely tested under load (e.g., with facility functions being served off of the generator in real-time, not just tested to see if it turns on)? ☐ No ☐ Yes If yes: ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Semi-Annually ☐ Annually *Describe*: _____ **Does the facility have Uninterrupted Power System (UPS)/Battery backup?** ☐ No ☐ Yes Purpose of UPS/Battery backup (check one): ☐ Life Safety ☐ Graceful shutdown ☐ Core Operations ☐ Entire Facility Load Duration of UPS/Battery backup _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) UPS/Battery backup configuration ☐ In addition to backup generator(s) ☐ To accommodate switch from external supply to backup generator(s) ☐ Sole backup for loss of external supply
Backup Generation Briefing Notes: _____	
Overall Electric Power Comments: _____	

UPS/Battery backup
Uninterruptible power supply or uninterruptible power source provides emergency power to a load when the main power source fails. Normally this equipment is used to bridge the time for the switch from the main electric power supply to an alternative source of electricity (usually diesel generators). Facilities that have very sensitive technologies may use battery rooms or banks that actually take the external power (whether from the utility or the backup generator) convert it from alternating current to direct current and then back to alternating current; sometimes called double-conversion systems. These can also serve as uninterruptible backup power.

UPS/Battery backup configuration

UPS can be central and stand-alone devices. This difference is not critical. However, central UPS provides a more integrated solution.

In addition to backup generator(s)
As an example, the UPS could keep cyber and communication systems operational, while the backup generator maintains lights and other building functions.

To accommodate switch from external supply to backup generator(s)
As an example, the UPS could maintain cyber and building systems for 1-15 minutes until the backup generator can be brought online and then would no longer be needed.

Sole backup for loss of external supply
As an example, core operations of the facility could be maintained on a UPS or battery system.

Dependencies – Natural Gas	
Natural Gas	Is external natural gas required for Facility core operations (e.g., produce key services/goods)? ☐ No ☐ Yes If yes, complete this section. Primary use for natural gas: *(Check all that apply)* ☐ On-site heat / hot water ☐ Food preparation ☐ Facility power ☐ Steam generation (cogeneration) ☐ Heat/Energy for Core Operations ☐ Used as a raw material (e.g., to produce ammonia, hydrogen, etc. Other, *Describe:* _____
Natural Gas External Sources	What is the name of the Natural Gas supplier: _____ How many natural gas service connections are there for the facility? ☐ One ☐ More Than One If more than one, can each service connection handle entire facility load? ☐ No ☐ Yes If there are multiple service lines, where do the lines enter the facility? ☐ Same location ☐ Different geographic locations *Describe*: _____ Service connections into the facility are located ☐ Aboveground ☐ Buried ☐ Mixed (both aboveground and buried)

DEPENDENCIES – NATURAL GAS

For natural gas, the question set captures only the external source. If **the facility does not receive any natural gas from an external source**, please **check NO and go to the next section: Dependencies – Water**

Service Connections
To determine the location of service connections, consider everything between where the service enters the facility's property line until it terminates at the facility's system (e.g., the meter on the outer wall of an office building or the internal manifold where external service ends and the facility's natural gas system begins).

Dependencies – Natural Gas	
Natural Gas External Sources	Are the main service lines collocated with other utilities (e.g., utility corridors with electric, Communications, fiber, water)? ☐ No ☐ Yes Components of the natural gas supply located inside the building (within control of facility) are protected from vandalism or accidental damage ☐ No ☐ Yes Components of the natural gas supply located outside of the building (but still within control of facility) are protected from vandalism or accidental damage ☐ No ☐ Yes
Natural Gas External Sources Briefing Notes: _____	

This page is intentionally left blank

Dependencies – Natural Gas	
Natural Gas Loss of Service	Has the facility experienced natural gas service outages within the last 5 years? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If external natural gas service is lost (without **considering any backup or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external natural gas is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after loss of natural gas including backup? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Natural Gas Loss of Service Briefing Notes: _____	

Is there a contingency/business continuity plan with provider for restoration
The intent of this question is to identify and describe specific service level or rate agreements that exist between the facility and the provider of natural gas.

Does the facility participate in provider priority plan for restoration
A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If external natural gas service is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted?
This question captures the impact of the worst case scenario, the fact that the facility loses natural gas and is unable to operate its backup.

Once external natural gas is lost (without considering any backup or alternative mode), what percentage of normal business functions would be lost or degraded?
This question captures impact of the worst case scenario, the fact that the facility losses natural gas and is unable to operate its backup.

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of natural gas. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of natural gas) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the external natural gas supply is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes such as relighting pilot lights (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external sources of natural gas. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of natural gas is lost during 7 days, what time will be needed for full resumption of core operations when the external sources of natural gas is restored.

Dependencies – Natural Gas	
Natural Gas Backup	Is there an internal natural gas source or an alternative fuel source (e.g., diesel fuel, propane or electricity) that can serve as a backup upon the loss of the primary natural gas source? ☐ No ☐ Yes If yes, *describe*: _____ Duration of backup: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external natural gas service is lost (**and your backup or alternative fuel is employed**), what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Natural Gas Backup Briefing Notes: _____	
Overall Natural Gas Comments: _____	

Backup Gas or alternative source
If the facility has an internal source of natural gas (e.g., natural gas compressor uses natural gas directly from the pipe for fueling pumps) it should be captured as backup to the loss of external natural gas service. This could also be when something is dual-fueled (e.g., a boiler) and if natural gas service is lost, the equipment can quickly switch to diesel fuel.

Duration of Backup
The amount of time the facility can operate the backup gas supply or alternate source, e.g., backup propane supply runs out. However, if the facility processes can be operated continuously using electricity (e.g., heating system), then duration can be 365 days.

Dependencies – Water	
Water	Is external water required for the Facility Core Operations (Produce Key Services, Goods)? ☐ No ☐ Yes If yes, complete this section. What is the purpose of water usage: *(Check all that apply)* ☐ Domestic (e.g., potable water) ☐ Core Operations (e.g., rinse waters, process water, fire protection for special areas) ☐ Cooling (e.g., cooling towers, HVAC) ☐ Other *Describe*: _____
External Sources	What is the name of the Water Provider: _____ How many water service connections are there for the facility? ☐ One ☐ More Than One If more than one, can each service connection handle entire facility load? ☐ No ☐ Yes If there are multiple service lines, where do the lines enter the facility? ☐ Same location ☐ Different geographic locations *Describe*: _____ Are the main service lines collocated with other utilities (e.g., utility corridors with electric, Communications, fiber)? ☐ No ☐ Yes

DEPENDENCIES – WATER

For Water, the question set captures both external and internal sources. However, the primary focus is on external source. Information about internal source is only collected because a facility that has both internal and external sources of water is more robust and thus theoretically more resilient. This also makes the facility less susceptible to cascading failures.

By definition for the IST/SAV methodology, if the facility does not have any external source of water, **the facility is determined not dependent on water**. The calculation of the Resilience Measurement Index incorporates this concept into the relative value system.

If **the facility does not receive any water from an external source** (all water is obtained internally), please **check NO below and go to the next section: Dependencies – Wastewater**

If part or all the water needed for the facility core operations is furnished by an external source, please provide the information requested in this section. This section is also used when a facility has both an external dependency and an internal source of water.

Dependencies – Water	
External Sources	Are components of the water service located inside of the building (but still within control of facility) protected from vandalism or accidental damage? ☐ No ☐ Yes *Describe:* _____ Are components of the water supply located outside of the building (but still within control of facility) are protected from vandalism or accidental damage? ☐ No ☐ Yes *Describe:* _____
Water External Source Briefing Notes: _____	

Dependencies – Water	
Internal Sources:	Does the facility have an internal source of water? ☐ No ☐ Yes If yes, complete this section. What is the type of Internal sources? ☐ Onsite wells ☐ Surface water *Describe:* _____ Do onsite sources produce enough water to handle full facility load? ☐ Yes ☐ No Percent of Demand: _____ *Duration*: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Water Internal Source Briefing Notes: _____	

Dependencies – Water	
Water Loss of External Service	Has the facility experienced external water service outages within the last 5 years? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider(s) for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration/ ☐ No ☐ Yes *Explain*: _____ If the external water service is lost **(without considering any backup or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external water service is lost (**without considering any backup or alternative mode**) what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after loss of water including backup? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Water Loss of External Service Briefing Notes: _____	

Contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of water.

Does the facility participate in provider priority plan for restoration
A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If the external water service is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses water and is unable to operate its backup.

Once external water service is lost (without considering any backup or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses water and is unable to operate its backup.

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of water. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of water) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

For example, a building could be closed if water is not available for fire suppression systems.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the external water supply is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external sources of water. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of water is lost during 7 days, what time will be needed for full resumption of core operations when the external sources of water is restored.

Dependencies – Water	
Water Alternates and Backup	Is there an alternate to the external source of water? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No percentage: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once water service is lost (**and considering your backup or alternative mode**) what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Is there onsite water storage? ☐ No ☐ Yes If yes, Quantity: _____ (circle: Gallons or Acre-Feet)
Water Alternate and Backup Briefing Notes: _____	
Overall Water Comments: _____	

Water Alternatives and Backup

This section captures alternatives and backups in place at the facility than can provide water in case of loss of the external source of water.

If water service is lost (and considering your backup or alternative mode) what percentage of normal business functions would be lost or degraded?

This question captures the facility's capability to operate in case of disruption in the external supply of water. This information should take into account internal sources or any other alternatives at the disposal of the facility for supplying water in case of failure of the primary external source.

Dependencies – Wastewater	
Wastewater	Does the facility require external wastewater discharge services for Core Operations (Produce Key Services, Goods)? ☐ No ☐ Yes If yes, complete this section. What is the primary use for wastewater discharge services: *(Check all that apply)* ☐ Domestic ☐ Industrial Wastewater ☐ Livestock ☐ Other *Describe*: _____
External Discharge Services:	What is the name of the Wastewater Receiver (e.g., Collection system or treatment plant): _____ How many wastewater laterals are there for the facility? ☐ One ☐ More than one If more than one, can each lateral handle entire facility load? ☐ No ☐ Yes If there are multiple laterals, where do the lines exit the facility? ☐ Same location ☐ Different geographic locations *Describe*: _____

DEPENDENCIES – WASTEWATER

For Wastewater, the question set captures both external and internal wastewater discharge services. However, the primary focus is on external service. Information about internal source is only collected because a facility that has both internal and external wastewater discharge services is more robust and thus theoretically more resilient. This also makes the facility less susceptible to cascading failures.

By definition for the IST/SAV methodology, if the facility does not have any external wastewater discharge service for wastewater, **the facility is determined not dependent on wastewater service**. The calculation of the Resilience Measurement Index incorporates this concept into the relative value system.

Then, if **the facility does not use an external wastewater discharge service** (all wastewater is treated internally), please **check No below and go to the next section: Dependencies – Communications**

If part or all the wastewater discharge service needed for the facility core operations is furnished by an external provider, please provide the information requested in this section. Also use this section when a facility has both an external dependency and an internal wastewater discharge service.

Check all primary wastewater discharge services that apply

In order to be a redundant wastewater system, the onsite treatment would have to be discharged via the facility's own discharge pipes directly to the ultimate receiving waters without needing the local wastewater provider (e.g., they have an individual EPA-issued National Pollutant Discharge Elimination System [NPDES] permit). If the internal water collection/treatment components discharge offsite to the local municipal or regional wastewater authority, then that type of internal system is not a redundant system because it cannot operate upon loss of the wastewater service provider. It may be that domestic sewage is discharged to the local or regional wastewater authority; however, industrial wastewater is treated onsite and discharged directly to a water body. Few facilities will have onsite domestic sewage treatment and discharge.

Dependencies – Wastewater	
External Discharge Services:	Are the main laterals collocated with other utilities (e.g., utility corridors with electric, Communications, fiber, water)? ☐ No ☐ Yes Components of the wastewater service located inside of the building (but still within control of facility) are protected from vandalism or accidental damage ☐ No ☐ Yes If Yes, describe: _____ Components of the wastewater service located outside of the building (but still within control of facility) are protected from vandalism or accidental damage ☐ No ☐ Yes If Yes, describe: _____
Wastewater External Discharge Services Briefing Notes: _____	

This page is intentionally left blank

Dependencies – Wastewater	
Internal Discharge Services:	Does the facility have an internal wastewater discharge service? ☐ No ☐ Yes What are the types of Internal discharge services? ☐ Onsite sewage treatment ☐ Industrial Wastewater treatment plant *Describe:* _____ Are onsite services sufficient to handle full facility wastewater load? ☐ Yes ☐ No If no, Percent of discharges: _____% *Duration*: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Wastewater Internal Discharge Services Briefing Notes: _____	

What are the types of Internal discharge services

Consider the service that can fully treat most of the wastewater load produced by the facility. If the internal service is only used for a pre-treatment, it should not be considered the primary wastewater discharge service.

In order to be a redundant wastewater removal system, the onsite treatment would have to be discharged via the facility's own discharge pipes directly to the ultimate receiving waters without needing the local wastewater provider (e.g., they have an individual EPA-issued National Pollutant Discharge Elimination System [NPDES] permit). If the internal wastewater collection/treatment components discharge offsite to the local or regional wastewater authority, then that type of internal system is not a redundant system because it cannot operate upon loss of the wastewater service provider. It may be that domestic sewage is discharged to the local or regional wastewater authority, however, industrial wastewater is treated onsite and discharged directly to a water body. Few facilities will have onsite domestic sewage treatment and discharge.

Dependencies – Wastewater	
Loss of External Wastewater Discharge Service	Has the facility experienced external wastewater service outages within the last year? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If the external wastewater service is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external wastewater service is lost (**without considering any backup or alternative**) what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after loss of wastewater discharge service including backup? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once external service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Wastewater Loss of External Service Briefing Notes: _____	

Is there a contingency/business continuity plan with provider for restoration?

The intent of this question is to define if specific service level agreements exist between the facility and the provider of wastewater removal service.

Does the facility participate in provider priority plan for restoration

A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If the external wastewater service is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario: the fact that the facility loses wastewater discharge service and is unable to operate its backup.

Once external wastewater service is lost (without considering any backup or alternative) what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario: the fact that the facility loses wastewater discharge service and is unable to operate its backup.

External regulation policy

The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of wastewater discharge services. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of wastewater treatment) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

For example, a building could be closed if connections to a wastewater removal/treatment system are not available for the disposal of sanitary water or the disposal of industrial wastewater.

Restoration time

The intent of this question is to determine the time needed for the facility to resume normal operations after the external wastewater system is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external wastewater discharge service. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external wastewater discharge service is lost during 7 days, what time will be needed for full resumption of core operations when the external wastewater discharge service is restored.

Dependencies – Wastewater	
Wastewater Alternate	Is there an alternate to the external wastewater discharge service? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No If no, Percent of Discharges: _____% Once external wastewater service is lost (**and considering your backup or alternative mode**) what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) What is the duration of this alternative _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days)
Wastewater Alternate Briefing Notes:_____	
Overall Wastewater Comments:_____	

Wastewater Alternate

This section captures alternatives and backups in place at the facility that can provide wastewater discharge services in case of loss of the external source of service.

If the external wastewater discharge service is lost (and your backup or alternative is implemented) what percentage of normal business functions are lost or degraded?

This question captures the facility's capability to operate in case of disruption in the external supply of wastewater discharge service. This information should take into account internal sources or any other alternatives at the disposal of the facility for dealing with wastewater discharge in case of failure of the primary external source.

Dependencies – Communications	
Communications (Focus on the infrastructure that supports voice and data communications for the facility)	Are external communications required for Facility core operations (e.g., produce key services/goods)? ☐ No ☐ Yes If yes, complete this section. Which of these communication services is critical to facility operations? (Check all that apply) ☐ Telephone ☐ Data (Includes networking and Voice-over IP) ☐ Radio Link Select one primary critical communications mode [mode the loss of which would result in the most severe impact to facility functions –only check one] ☐ Telephone ☐ Data (Includes networking and Voice-over IP) ☐ Radio Link **Complete the follow-on questions only for the primary critical communications mode/service selected above.**
Telephone Mode	
Primary Critical Telephone Usage	☐ General business or administration or customer services function (General) ☐ Command, control, interrogation & monitoring of equipment and processes (SCADA/PCS) ☐ Dispatch functions (Dispatch)
Data Mode (e.g., fiber cable)	
Primary Critical Data Services Usage	☐ General business or administration or customer services function (General) ☐ Command, control, interrogation & monitoring of equipment and processes (SCADA/PCS) ☐ Dispatch functions (Dispatch)
Radio Mode (e.g., microwave or radio tower)	
Primary Critical Radio Usage	☐ General business or administration or customer services function (General) ☐ Command, control, interrogation & monitoring of equipment and processes (SCADA) ☐ Dispatch functions (Dispatch)

DEPENDENCIES – COMMUNICATIONS

For Communications, the questions set capture only the external source. If **the facility does not receive any communications service from an external source, please check No below and go to the next section: Dependencies – Information Technology.**

Communication Modes

Telephone: Telephone service includes hard-wired (e.g., landline) or fixed location desktop or wall telephone. It can include a portable phone that uses a base that is hard-wired. IT DOES NOT INCLUDE CELL PHONES.

Data: Data service includes hard-wired (e.g., fiber) or fixed locations that enter the facility at communication rooms, closets or the initial connection to facility IT equipment. It does not include mobile or wireless laptops or remote units. It does include voice-over-IP. For data, the Communications Dependency section covers the link for the both SCADA and business system to the outside carrier (e.g., Comcast or AT&T).

The IT Dependency section will cover the policies and protections of the IT data system once the link has been made.

Radio Link: Radio Link includes any voice or data transmission from a device that is NOT hard-wired (e.g., transmission over radio frequencies, including cell phones, 800 MHz radios, Blackberries, walkie-talkie and microwave units).

Complete the follow-on questions only for the primary critical communications mode/service selected above. Work with the Owner/Operator to determine which of the communication modes and which of the communication services is most important to the operation of the facility. This may be difficult to decide if the control system or the business system is more important, however try to think of what will cause facility operations/function to cease or be degraded rather than impacts to a facility's ability to carry on administrative functions. Also, it may be that they rely on multiple modes to carry out this communication service (e.g., cell phones and radios), but only one can be the primary critical communication mode.

Dependencies – Communications	
Protective Measures For Primary Critical Communications Mode and Service **[For example, Telephone is the Mode and General Business is the Service; or Data is the Mode and Control is the Service]**	What protective measures are employed for the primary communication service? (Check all that apply) ☐ More than one service connection (e.g., telephone line, data cable or radio tower) at the facility ☐ If more than one service connection, they are in different geo-locations ☐ More than one inside terminal/Communications room ☐ Service connections are located underground ☐ Service connections terminate in a protected facility/building ☐ Service connections are not located in a joint, co-located utility corridor ☐ None
Communications Service Briefing Notes: _____	

This page is intentionally left blank

Dependencies – Communications	
Impact of loss of Primary Communication Mode and Service (cont'd)	Has the facility experienced communication service outages within the last year? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If external communication service is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once the facility has lost external communication service mode (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after loss of communications including backup? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Communications Impact of Loss of Service Briefing Notes: _____	

Is there a contingency/business continuity plan with provider for restoration
The intent of this question is to identify and describe specific service level or rate agreements that exist between the facility and the utility/service/product provider.

Does the facility participate in provider priority plan for restoration
A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore services to them before other customers.

If external communication service is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted:
This question captures the impact of the worst-case scenario: the fact that the facility loses communications provided by an external supplier and is unable to operate its backup.

Once the facility has lost communication service mode (without considering any backup or alternative mode), what percentage of normal business functions are lost or degraded?
This question captures impact of the worst-case scenario, the fact that the facility losses communications provided by an external supplier and is unable to operate its backup.

External regulation policy
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of communications. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of communication) after a c ertain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively. For example, a building may need to shut down if it is impossible to have access to 911 services. In fact this question relates directly to the Maximum Tolerable Time of Degradation as well as the tolerable level of degradation.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the external communication supply is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of communications. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of communications is lost during 7 days, what time will be needed for full resumption of core operations when communications are restored.

Dependencies – Communications	
Communications Alternate and Backup	If primary mode of communication service is lost, is there a backup mode of communication? ☐ No ☐ Yes Duration of backup: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once the facility has lost external communication service mode (**and your backup or alternative is implemented**) what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Communications Alternate and Backup Briefing Notes: _____	
Overall Communications Comments: _____	

Communications Alternate and Backup
Backup Communications should be a different mode than the primary mode. For instance, if the facility's primary mode was telephone; they would normally have a different mode (e.g., radio) for communications. However, for instance, if the facility possesses its own communication system, it can be captured as backup to the primary, outside system. The capability to operate manually is another example of alternate to the loss of communications.

Duration of Backup
The amount of time the facility can operate the backup mode of communication, e.g., radios. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Information Technology	
Is Information Technology required for Facility core operations (e.g., produce key services/goods)? ☐ No ☐ Yes If yes, complete the following section.	
Information Technology Management	
Resilience Operations	Is there a manager/department in charge of IT security management? ☐ No ☐ Yes If yes, is this the primary function of that manager/department? ☐ No ☐ Yes
IT Sources	What type of IT do you use? (check all that apply) ☐ Internet ☐ Internal IT What is the name of the IT provider/supplier: _____ **Critical Uses for IT Service:** (Check all that apply) ☐ Business Network General business or administration or customer services function (e.g., taking/filling orders, patient records) (Business Network) *Describe*: _____ ☐ Control Network ☐ Supervisory Control and Data Acquisition (SCADA) *Describe*: _____ ☐ Process Control Systems (PCS) *Describe*: _____

DEPENDENCIES – INFORMATION TECHNOLOGY

The Communications Dependencies section covers the linkage for the both SCADA and business systems to the outside carrier. The Information Technology (IT) Dependencies section covers the policies and protections of the IT data system once the linkage has been made.

Note: Questions have been developed and added in collaboration with the Cyber Resilience Review (CRR) team of the DHS National Cybersecurity Division. Answer to these questions provide information that will be used "to understand whether the organization (interviewed) participates in cybersecurity information sharing, has critical cyber dependencies, and uses community resources for cybersecurity management.

Is Information Technology required for Facility core operations (e.g., produce key services/goods)?
Answer to this question is YES is the facility primary mission(s) depend(s) on information technology assets to be functioning and in good working order.

If the facility does not need IT for supporting its core operations, **please check No and go to the next section: Dependencies – Transportation.**

Critical Uses for IT Service

Business Network
A business network includes email, billing, file storage, etc. It may perform general business, administration, or customer service (e.g., taking/filling orders, patient records) functions.

Control Network
Control networks relate to systems that are used to manage the control of operations, e.g., opening valves to control gas flow, measuring water flow at a water treatment facility, controlling package sorting at a shipping facility, etc.

Complete the follow-on questions only for the primary critical IT mode/service selected (Internet or Internal IT). Work with the Owner/Operator to determine which of the IT modes and which of the IT services is most important to the operation of the facility. This may be difficult to decide or even determine if the control system or the business system is more important, however try to think of what will cause facility operations/function to cease or be degraded rather than impacts to a facility's ability to carry on administrative functions. Also, it may be that they rely on multiple modes to carry out this IT service, but only one can be the primary critical IT mode. If both are critical, simply pick one of them and answer accordingly.

Dependencies – Information Technology	
Does the facility report cybersecurity incidents to outside organizations?	☐ No ☐ Yes If yes, for what purpose do you make such reports: ☐ Request technical assistance (U.S. CERT, IRT teams, etc.) ☐ Request incident management support ☐ Regulatory (e.g., NERC CIP)? ☐ Information sharing (e.g., U.S. Cert, state computer security incident response teams, fusion centers) ☐ Law enforcement (e.g., FBI, USSS, state/local police) Describe: _____
Does anyone from the facility actively participate in local or regional cybersecurity forums (e.g., exchange lessons learned, best practices, training)?	☐ No ☐ Yes If yes, please list and describe. ☐ Sector-specific information sharing and analysis center. Which one(s)? _____ ☐ Sector-related associations/partnerships Which one(s)? _____ ☐ Federal or State-led partnerships (e.g., FBI InfraGard chapter(s)) Which ones? _____ ☐ Fusion center(s) Which one(s)? _____ ☐ State or local law enforcement department(s) Which one(s)? _____ ☐ State or local IT office(s) Which one(s)? _____ ☐ Other(s) Describe: _____

Does the facility report cybersecurity incidents to outside organization?
Organizations have varying criteria for declaring a cyber security incident. However, in general terms, a cybersecurity incident is an event that violates written or implied security policies. Depending on the organization, examples might include spear phishing campaigns, stolen data, and denial service attacks.

Dependencies – Information Technology	
Does the facility receive threat and vulnerability information, cybersecurity-related bulletins, advisories, and alerts from an external source?	☐ No ☐ Yes If yes, ☐ DHS US-CERT ☐ DHS ICS-CERT ☐ DHS Open Source Enterprise (OSE) Daily Cyber Report ☐ DHS Daily Open Source Infrastructure Report ☐ DHS Homeland Security Information Network (HSIN) ☐ SANS Internet Storm Center ☐ Vendors ☐ State or local law enforcement departments(s) ☐ Other Which one(s)? _____ How often do you receive this information? ☐ Daily ☐ Weekly ☐ Monthly
Does the facility utilize formal, external cybersecurity guidance and standards for identifying and implementing cybersecurity controls (management, operational, and technical) (e.g., NIST Special Publications 800-series, ISO/IEC 27001, CoBIT, ITIL)?	☐ No ☐Yes Which guidance or standard? _____
Does the facility perform threat monitoring and/or threat management/remediation?	☐ No ☐ Yes Is this function performed by a third-party contractor? ☐ No ☐ Yes What is the name of the contractor: _____ Describe: _____

Does the facility utilize formal, external cybersecurity guidance and standards for identifying and implementing cybersecurity controls (management, operational, and technical) (e.g., NIST Special Publications 800-series, ISO/IEC 27001, CoBIT, ITIL)?
This question captures if the facility utilizes stantards to develop policies regarding cyber security. This includes policies that affect people, processes, and equipment.

Does the facility perform or utilize threat monitoring and/or threat management/remediation?
Is this function performed by a third-party contractor?
Some organizations will hire a third party to provide them with cyber threat and vulnerability information as well as real-time system monitoring services. Some examples include Dell Secure works, Symantec, NEC, IBM and many others.

Dependencies – Information Technology	
Does the facility have an IT service provider or an internal cyber team responsible for immediately responding to, coordinating, and/or managing cyber incidents?	☐ No ☐ Yes Is this service provider or team capable of initiating response and managing a cyber emergency? ☐ No ☐ Yes Without external partners? ☐ No ☐ Yes
Does the facility rely upon a local or regional partner – such as fusion center, law enforcement department, private sector partner, and state or local government offices - for IT business continuity, IT disaster recovery, event management, regional catastrophic recovery, or operational response?	☐ No ☐ Yes ☐ Sector-specific information sharing and analysis center. Which one(s)? _____ ☐ Sector-related associations/partnerships Which one(s)? _____ ☐ Federal or State-led partnerships (e.g., FBI InfraGard chapter(s)) Which ones? _____ ☐ Fusion center(s) Which one(s)? _____ ☐ State or local law enforcement department(s) Which one(s)? _____ ☐ State or local IT office(s) Which one(s)? _____ ☐ Other(s) Describe _____

Does the facility have an IT service provider or an internal cyber team responsible for immediately responding to, coordinating, and/or managing cyber incidents?
Some facilities hire an external third party to monitor their IT networks and respond to cyber security threats and incidents. Alternatively, larger organizations may opt to build an internal team comprised of IT and IT security professionals trained to perform this function. Some responsibilities of these providers and teams include Intrusion Detection / Prevention (IDS/IPS), virus/malware detection, and incident response.

Does the facility rely upon a local or regional partner – such as fusion center, law enforcement department, private sector partner, and state or local government offices - for IT business continuity, IT disaster recovery, event management, regional catastrophic recovery, or operational response?
The organization has relationships with regional partners to provide assistance in the form of information, technical expertise, emergency coordination, potential relocation and/or restoration resources.

Dependencies – Information Technology	
Does the organization have a Cybersecurity Plan?	☐ Yes ☐ No *If yes,* The plan is developed at the: ☐ Corporate-level ☐ Facility-level ☐ IT Service-level Has the plan been approved by senior management? ☐ Yes ☐ No Is the plan required by a Federal, state, or local regulation? ☐ No ☐ Yes Is the plan reviewed at least annually? ☐ Yes ☐ No Are key personnel aware of and do they have access to a copy of the plan? ☐ Yes ☐ No Are personnel trained on the plan? ☐ No ☐ Yes If yes, ☐ Key personnel only are trained on the plan *(Check all that apply)* ☐ At initial employment ☐ At least once a year Or, ☐ All personnel are trained on the plan *(Check all that apply)* ☐ At initial employment ☐ At least once a year

Does the organization have a Cybersecurity Plan?
The answer to this question should be " YES" if the facility has documentation that addresses cybersecurity or IT service continuity. IT service involves addressing continuity of operations, business continuity, IT disaster recovery, etc. These plans may exist separately or could be included in the organizations overall plans but should address IT specifically.

Are personnel trained on the plan?
The intent of this question is to capture if the personnel know the plan and its content (procedures), and their role in the case of an incident.

Dependencies – Information Technology	
Does the organization have a Cybersecurity Plan?	Does the Cybersecurity Plan address: ☐ Identification and classification of cyber critical assets ☐ Access control policies ☐ IT security roles and responsibilities ☐ IT security training ☐ Audit Trails ☐ Disposal of protected assets ☐ Incident Response/Management ☐ Unauthorized Access ☐ Denial of Service ☐ Malicious Code ☐ Improper Usage ☐ Scan/Probes/Attempted Access ☐ Security testing ☐ Physical security of critical IT assets ☐ Fire walls ☐ Electronic communications ☐ Remote access ☐ Is not allowed ☐ Is allowed only when needed, then access disabled (physically or electronically) ☐ Is allowed at all times ☐ user controls are in place Is remote access allowed to continue operations during circumstances that may preclude access to the facility (e.g., hurricane aftermath or pandemic situations)? ☐ Yes ☐ No ☐ Wireless ☐ Is not allowed ☐ Is allowed on private network space (requires authentication / WEPkey, etc. to gain access) ☐ Is allowed on guest network only ☐ Is allowed, open to all, with access to company network ☐ Security patches or updates ☐ None of the above

Incident Response/Management
This element captures the means of the facility to detect and respond to five categories of cyber incidents: Unauthorized Access, Denial of Service (DOS), Malicious Code, Improper Usage and Scans/Probes/Attempted Access. The incidents listed can be detected by multiple technical means including Intrusion Detection/Prevention systems (IDS/IPS), firewalls, anti-virus tools, and vulnerability detection/assessment tools.

Unauthorized access: an individual gains logical or physical access without permission to a network, system, application, data, or other resource.

Denial of Service (DOS): An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DOS.

Malicious code: successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.

Improper usage: a person violates acceptable computing use policies.

Scans/Probes/Attempted Access: any activity that seeks to access or identify a computer, open parts, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

Remote Access
Remote Access allows connectivity to the internal network from the outside. User controls can include only allowing designated users to connect remotely, vs. all users; use of secure tokens; changing default passwords on remote devices; etc.

Wireless
Wireless connectivity introduces additional security concerns. A best-case scenario would be for wireless to not be used at all, especially on control networks. Other scenarios may have a separate visitor network space, such that a visitor would not be able to scan traffic on the internal network. Employees would need to VPN or authenticate in some manner to gain access. A worst-case scenario would be that wireless is open to all, and exists on the same network as the internal systems.

Dependencies – Information Technology	
Does the organization have a Cybersecurity Plan?	Does the facility conduct cybersecurity exercises for purposes of training, system testing, continuity planning, or disaster recovery? ☐ No ☐ Yes When: _____ The plan is exercised at least once a year ☐ No ☐ Yes If yes, these exercises are: ☐ Tabletop (practical or simulated exercise) ☐ Functional (specialized exercise) ☐ Full scale (simulated or actual event)) Are exercise results documented, approved and reported to executive management? ☐ No ☐ Yes
Administration Policy	Has a cybersecurity assessment been completed? ☐ No ☐ Yes ☐ Internal Assessment How often? ☐ 6 months ☐ Annually ☐ Less frequently than annually ☐ External Assessment How often? ☐ 6 months ☐ Annually ☐ Less frequently than annually Describe: _____
	Are security scans performed? ☐ No ☐ Yes If yes, How often? ☐ Continuously via active system /IDS (to detect and isolate threats) ☐ Every 3-6 months ☐ Annually ☐ Less frequently than annually
Information Technology Management Briefing Notes: _____	
Overall IT Management Comments: _____	

Has a cyber assessment been completed?
An assessment of a cybersecurity stature involves auditing the systems, policies, and procedures within an organization, in addition to performing a risk assessment. This allows an organization to identify their critical systems, develop a plan for disaster recovery, establish policies for user controls, and create short and long term direction for the computing environment. A cybersecurity plan can be the resulting document of this assessment. The following site can provide further information. http://www.sans.org/reading_room/whitepapers/auditing/an_overview_of_threat_and_risk_assessment_76.pdf.

Security scans are performed for vulnerabilities
Vulnerabilities include software holes that a hacker might take advantage of, out of date virus definition files, default passwords set by a vendor, or accounts that are not password protected. Software designed for scanning, such as ISS or Nessus, is commonly used, as is active scan systems, which detect vulnerabilities as soon as a system joins the network.

Dependencies – Information Technology

Does the facility have a control and business network?
☐No
☐Yes

If yes, is there network segmentation between control networks and business networks?
☐No
☐Yes

Are there redundant separated critical servers or network components?
☐ No
☐ Yes

Does the facility use Backup Data Storage?
☐ No
☐ Yes

How often are backups performed?
☐ Daily
☐ Weekly
☐ Monthly

Are data restores performed and verified (e.g., backup data is restored and checked to see if it works)?
☐ No
☐ Yes

Is access to control/computer rooms and remote equipment controlled?
☐ No
☐ Yes
If yes, describe: _____

Are there redundant, separated critical servers or network components?

This will occur when systems are redundant and are in different rooms or buildings or are a reasonably significant distance apart.

Does the facility use Backup Data Storage?

This question captures if the facility has procedures for data backup and the storage of those data. This is different from the information captured in the business continuity plan section, and it is not intended to capture if the facility has an alternative data center. That information should be captured in the alternative site section. For example, this section will capture a hospital's capability to store electronic medical records at another location for later restoration of the original database/system.

Dependencies – Information Technology	
Information Technology Loss of Service	Is there a contingency/business continuity agreement with the provider for restoration? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in a provider priority plan for restoration? ☐ No ☐ Yes If the information technology system is lost completely (**and no backup is employed**), within what time period would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once the information technology system is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline) Are there external regulations/policies that mandate the facility shut down after loss of information technology service including backup? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____
Information Loss of Service **Briefing Notes:** _____	

Contingency/business continuity plan with provider for restoration
The intent of this question is to identify and describe specific service level or special rate agreements that exist between the facility and the utility/service/product provider.

Does the facility participate in provider priority plan for restoration
A priority plan is a "list" of facilities or types of facilities that will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If the information technology system is lost completely (and no backup is employed), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario: the fact that the facility completely loses its IT system and is unable to operate its backup.

Once the information technology system is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded?

This question captures the impact of the worst case scenario: the fact that the facility completely loses its IT system and is unable to operate its backup.

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of information technology service. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of information technology) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively. In fact this question relates directly to the Maximum Tolerable Time of Degradation as well as the tolerable level of degradation.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the information technology service is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of information technology. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of information technology is lost during 7 days, what time will be needed for full resumption of core operations when information technology service is restored.

Dependencies – Information Technology	
Information Technology Alternate	If information technology service is lost, is there an alternative or backup mode? ☐ No ☐ Yes If yes, describe: Duration of alternative: _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once the information technology system is lost (**and considering your backup or alternative mode**) what percentage of normal business functions are lost or degraded? ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Information Technology Alternate and backup **Briefing Notes:** _____	
Overall Information Technology **Comments:** _____	

IT Alternate and Backup
Several types of alternative or backup can be in place (e.g., telephone, radio/satellite link. alternate site). A Secondary Site could take over functionality, either automatically or by flipping a switch, from the primary site should there be a major loss at the primary. The capability to operate manually is another example of alternate to the loss of IT services (e.g., paper order forms).

Duration of alternative
The amount of time the facility can operate the backup to internet, e.g., DSL connection. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Once the facility is on backup mode, what percentage of normal functions are lost or degraded?
This question must be answered only if the facility has a backup mode for Internet.

Dependencies – Transportation	
Is Transportation required for the Facility Core Operations (Produce Key Services, Goods)?	☐ No ☐ Yes If yes, please answer the following questions
Dependencies – Rail Transportation	
Mode: Rail (including bridges and tunnels)	Disruption of rail transport would cause a significant disruption to facility operations? ☐ No ☐ Yes *List critical transportation asset(s)*: _____ Why is rail transportation critical to facility operations? ☐ Work force arrival/departure Explain: _____ ☐ Receipt of critical materials/services ☐ Shipment of products ☐ Disposal of byproducts/wastes What is the name of the company that provides this service: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes Explain: _____ If all rail service is lost (**without considering any redundant or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once rail service is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

DEPENDENCIES – TRANSPORTATION

For each critical transportation mode, list transportation assets critical to providing that particular transportation mode. For instance, if the facility is dependent on rail transportation for receipt of critical materials, the CSX siding running into the facility clearly would be a critical asset, however, if the siding is dependent in turn on a nearby CSX rail bridge that, too, could be listed as a critical asset. You may list as many critical transportation assets per transportation mode as you wish; however, the questions on criticality and redundancy (alternative mode) are answered only for the transportation mode as a whole. Whether the siding or the bridge is lost, the facility still has no rail service; so, answer those questions as if the facility has no rail service.

The transportation section is designed to find a single point of failure that essentially isolates a given facility; it is not used to address all roads leading to the facility. transportation is only considered a dependency if a transportation asset or mode is essentially a single point of failure (e.g., a bridge leading to a site would be considered a dependency if there is no alternative route to the site and loss of the bridge would impact the site's core business functions; or, freight rail would be considered a dependency if, without this service, a site was not able to continue core business functions because of a lack of alternative transportation modes).

Examples of transportation dependencies:

- A large power generating facility that receives coal via a rail spur (replacing that much coal by truck is not practical).
- Any island facility will likely have a maritime dependency if the raw products are brought in by ship.
- A petroleum refinery that receives crude oil as a raw material may rely on one maritime channel.

The question set considers five types of transportation dependencies

- Rail Transportation,
- Air Transportation,
- Road Transportation,
- Maritime Transportation, and
- Pipeline Transportation.

If one of these modes of transportation constitutes a single point of failure for the facility core operations, please provide the information requested in this section. If this is not the case, please **check No below and go to the next section: Dependencies – Critical Products.**

Is Transportation required for the facility core operations (production of key services, goods)?

A dependency on a mode of transportation is identifies single points of failure in the transportation system that would severely impact the operability of the facility. For instance, this section does not address all roads leading to the facility; if there are multiple public road routes to reach the facility, the facility is not dependent on a single road, so select NO. Facilities that would be dependent on the road mode of transportation would be those where access is limited to one or two bridges/tunnels, the loss of which would isolate the facility. In urban areas, this would be rare. In rural areas, a long private-access road could create a dependency on road mode of transportation; such a dependency road mode of transportation could be for commuting personnel, as well as delivery or shipment of products or wastes.

This applies to all transportation modes. Occasionally, but rarely, a facility is dependent upon a particular transportation mode, and there may be a single point of failure. An example is a power-generating plant that receives all its coal via rail only. It would be impossible to ship the necessary amount of coal via road or other transportation mode. There is a single siding that comes into the facility, and one mile away there is a rail bridge that, if lost, isolates the facility. In this case, the facility does have a rail dependency. Very few places are dependent on air, however, some facilities on islands or a location like Juneau, Alaska, may have a dependency on air and/or maritime.

This page is intentionally left blank

Mode: Rail (including bridges and tunnels)

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If all rail service is lost (without considering any redundant or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses essential rail service and is unable to use a redundant or alternative mode.

Once rail service is lost (without considering any redundant or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses essential rail service and is unable to use a redundant or alternative mode.

Dependencies – Rail Transportation	
Mode: Rail (including bridges and tunnels)	Are there external regulations/policies that mandate the facility shut down after loss of rail service? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once rail service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Are there alternative modes of transportation in case of loss of rail transportation? ☐ No ☐ Yes Describe alternative mode of transportation: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once rail service is lost (**and your redundant or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Rail Transportation Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of rail transportation. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to use its alternative to rail transportation after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the rail transportation is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of rail transportation. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if rail transportation is lost during 7 days, what time will be needed for full resumption of core operations when rail transportation is restored.

What is the duration of this alternative?
In most cases, alternatives implemented for transportation can last indefinitely. For example, road transportation can be used as alternative to rail transportation. However, it is possible that a facility has an alternative that would not be efficient for a long period of time. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Air Transportation	
Mode: Air	Disruption of air transport would cause a significant disruption to facility operations? ☐ No ☐ Yes *List critical transportation asset(s)*: _____ Why is air transportation critical to facility operations? ☐ Work force arrival/departure Explain: _____ ☐ Receipt of critical materials/services ☐ Shipment of products ☐ Disposal of byproducts/wastes What is the name of the company that provides this service: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes Explain: _____ If all air service is lost (**without considering any redundant or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once air service is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Mode: Air

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If all air service is lost (without considering any redundant or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses essential air service and is unable to use a redundant or alternative mode.

Once air service is lost (without considering any redundant or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses essential air service and is unable to use a redundant or alternative mode.

Dependencies – Air Transportation	
Mode: Air	Are there external regulations/policies that mandate the facility shut down after loss of air service? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once air service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Are there alternative modes of transportation in case of loss of air transportation? ☐ No ☐ Yes Describe alternative mode of transportation: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once air service is lost (**and your redundant or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Air Transportation Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of air transportation. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to use its alternative to air transportation after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the air transportation is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of air transportation. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if air transportation is lost during 7 days, what time will be needed for full resumption of core operations when air transportation is restored.

What is the duration of this alternative?
In most cases, alternatives implemented for transportation can last indefinitely. For example, ground transportation can be used as alternative to air transportation. However, it is possible that this alternative would not be efficient in term of business for a long period of time. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Road Transportation	
Mode: Road (including bridges and tunnels)	Disruption of road transport would cause a s ignificant disruption to facility operations? ☐ No ☐ Yes *List critical transportation asset(s)*: _____ Why is road transportation critical to facility operations? ☐ Work force arrival/departure (other than mass transit): Explain: _____ ☐ Receipt of critical materials/services ☐ Shipment of products/services ☐ Disposal of byproducts/wastes Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes Explain: _____ If all road service is lost (**without considering any redundant or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once road service is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Mode: Road (including bridges and tunnels)

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If all road service is lost (without considering any redundant or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses essential road service and is unable to use a redundant or alternative mode.

Once road service is lost (without considering any redundant or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses essential road service and is unable to use a redundant or alternative mode.

Dependencies – Transportation	
Mode: Road (including bridges and tunnels)	Are there external regulations/policies that mandate the facility shut down after loss of access road? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once road service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Are there alternative modes of transportation in case of loss of road transportation? ☐ No ☐ Yes Describe alternative mode of transportation: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once road access is lost (**and your redundant or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Road Transportation Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of road transportation. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to use its alternative to road transportation after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the road transportation is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of road transportation. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if road transportation is lost during 7 days, what time will be needed for full resumption of core operations when road transportation is restored.

What is the duration of this alternative?
In most cases, alternatives implemented for transportation can last indefinitely. However, it is possible that this alternative would not be efficient in term of business for a long period of time. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Maritime Transportation	
Mode: Maritime	Disruption of maritime transport would cause a significant disruption to facility operations? ☐ No ☐ Yes *List critical transportation asset(s)*: _____ Why is maritime transportation critical to facility operations: ☐ Work force arrival/departure (e.g., ferry) *Explain:* _____ ☐ Receipt of critical materials/services ☐ Shipment of products/services ☐ Disposal of byproducts/wastes What is the name of the company that provides this service: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes Explain: _____ If all maritime service is lost (**without considering any redundant or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once maritime service is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Mode: Maritime

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If all maritime service is lost (without considering any redundant or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses essential maritime service and is unable to use a redundant or alternative mode.

Once maritime service is lost (without considering any redundant or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses essential maritime service and is unable to use a redundant or alternative mode.

Dependencies – Maritime Transportation	
Mode: Maritime	Are there external regulations/policies that mandate the facility shut down after loss of maritime service? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once maritime service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Are there alternative modes of transportation in case of loss of maritime transportation? ☐ No ☐ Yes Describe alternative mode of transportation: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once maritime service is lost (**and your redundant or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100%
Maritime Transportation Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of maritime transportation. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to use its alternative to maritime transportation after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the maritime transportation is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or security verifications (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of maritime transportation. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if maritime transportation is lost during 7 days, what time will be needed for full resumption of core operations when maritime transportation is restored.

What is the duration of this alternative?
In most cases, alternatives implemented for transportation can last indefinitely. However, it is possible that this alternative would not be efficient in term of business for a long period of time. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Pipeline Transportation	
Mode: Pipeline	Disruption of pipeline transport would cause a significant disruption to facility operations? ☐ No ☐ Yes *List critical transportation asset(s)*: _____ Why is pipeline transport critical to facility operations? ☐ Receipt of critical materials/services ☐ Shipment of products/services ☐ Disposal of byproducts/wastes What is the name of the company that provides this service: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes Explain: _____ If all pipeline transport is lost (**without considering any redundant or alternative mode**), how soon would the facility be severely impacted? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once pipeline service is lost (**without considering any redundant or alternative mode**), what percentage of normal business functions are lost or degraded? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Mode: Pipeline

Pipeline mode of transportation is only for pipelines that directly serve the facility and that are not captured in other dependency sections (e.g., natural gas or water). This section would not cover the pipelines that deliver natural gas from the local natural gas provider to the facility (that is covered in Natural Gas dependency). This would cover delivery of critical products and shipment of outgoing products by pipeline (e.g., crude oil in, refined product out, hydrogen as a raw material).

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If all pipeline transport is lost (without considering any redundant or alternative mode), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses essential pipeline service and is unable to use a redundant or alternative mode.

Once pipeline service is lost (without considering any redundant or alternative mode), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses essential pipeline service and is unable to use a redundant or alternative mode.

Dependencies – Pipeline Transportation	
Mode: Pipeline	Are there external regulations/policies that mandate the facility shut down after loss of pipeline service? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once pipeline service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Are there alternative modes of transport in case of loss of pipeline transportation? ☐ No ☐ Yes Describe alternative mode of transportation: _____ What is the duration of this alternative? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once pipeline service is lost (**and your redundant or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)
Pipeline Transportation Briefing Notes: _____	
Overall Transportation Comments: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of pipeline transportation. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to use its alternative to pipeline transportation after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the pipeline transportation is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or testing requirements (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of pipeline transportation. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if pipeline transportation is lost during 7 days, what time will be needed for full resumption of core operations when pipeline transportation is restored.

What is the duration of this alternative?
In most cases, alternatives implemented for transportation can last indefinitely. For example, ground transportation can be used as alternative to pipeline transportation. Crude oil and hydrogen can be transported via trucks or rail. However, it is possible that this alternative would not be efficient over a long period of time. If the facility can be fully operational continuously using this backup mode, then duration can be 365 days.

Dependencies – Critical Products	
Are Critical Products required for the Facility Core Operations (Produce Key Services, Goods)?	☐ No ☐ Yes If yes, please answer the following questions
Dependencies – Critical Products - Chemicals	
Chemicals	Does the facility use Chemicals (e.g., nitrogen, hydrogen, chlorine) for its core operations? ☐ No ☐ Yes *List:* _____ What chemical is the most critical to core operations? _____ **For the most critical chemical answer the following:** Is the most critical chemical available from multiple suppliers? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider(s)? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If critical chemical source(s) is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical chemical source(s) is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded: ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

DEPENDENCIES – CRITICAL PRODUCTS

General

The question set considers four types of Critical Products

- Chemicals,
- Fuels,
- Byproducts/wastes, and
- Raw materials.

If one of these products is critical for the facility core operations, please provide the information asked in this section. If this is not the case, please **check NO and go to the next section: Commendables.**

For Critical Products in each category, list only those that are absolutely necessary for the functioning of the facility. You may list as many as you like, however, the redundancy and consequence questions are to be answered for the category in general. For instance, the company may have five chemicals that are critical to operations, three are sole source.

For deciding if a product comes from a sole source supplier, determine if the facility has a sole-source contract with one supplier (i.e., at this time the facility does not receive the product or service from anyone other supplier) such that the loss of the supplier will impact the facility, then mark “Yes”. If other competitors or similar companies can provide the product or service then even if the supplier is lost the facility could continue to receive the product or service, but may experience a price impact (e.g., the supplier was the lowest bidder in supplying chlorine to the facility) or delivery delays (e.g., a new contract must be negotiated with the suppliers competitor before deliveries may commence), then mark “No”.

When answering if there are contingency/business continuity plans with the providers of all the chemicals, consider only those for which such a plan would be necessary. For instance, they use small quantities of a commonly available chemical for which there are many sources and no contract is in place, then a plan may not be necessary. If all chemicals for which a plan is necessary/prudent are in place, mark yes. If not, mark no.

For onsite storage, consider all critical chemicals listed when deciding if they have onsite storage and whether it is sufficient to support full core operations. To determine the duration of onsite storage support, consider the product with the shortest duration.

For the consequence questions (i.e., how soon would the facility be severely impacted and what percentage of normal business functions are lost or degraded), consider the product with the quickest and most severe consequence.

Critical Products – Chemicals

Please, do not fill in this section if chemicals are not provided by an external provider.

Is there a contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of Chemicals.

This page is intentionally left blank

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If critical chemical source(s) is lost (without considering any backup or alternative source), how soon would the facility be severely impacted?
This question captures the impact of the worst case scenario, the fact that the facility loses access to critical chemical source(s) and is unable to use a backup or alternative source.

Once critical chemical source(s) is lost (without considering any backup or alternative source), what percentage of normal business functions would be lost or degraded?
This question captures the impact of the worst case scenario, the fact that the facility loses access to critical chemical source(s) and is unable to use a backup or alternative source.

Dependencies – Critical Products - Chemicals	
Chemicals	Are there external regulations/policies that mandate the facility shut down after loss of main chemicals supply including alternate? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Is there an alternate (e.g., onsite storage) to the source of chemicals? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No percentage: _____ What is the duration of this alternative _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical chemical source(s) is lost (**and considering your backup or alternative mode (including the storage)**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)
Critical Products Chemical Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of critical chemicals. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup (without the primary source of chemicals) after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the external chemicals supply is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or testing requirements (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external sources of chemicals. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of chemicals is lost during 7 days, what time will be needed for full resumption of core operations when the external sources of chemicals is restored.

What is the duration of this alternative?
If the alternative considered is a s torage, please consider the duration of this storage without replenishing.

Dependencies – Critical Products - Fuels	
Fuels not including fuel for backup generators (e.g., diesel, gasoline, Aviation fuel)	Does the facility use **fuels (**e.g., diesel, gasoline, aviation fuel) **other than for backup generators** for core operations? ☐ No ☐ Yes *List*: _____ What type of fuel is the most critical to core operations? _____ **For the most critical fuel answer the following:** Is the most critical fuel available from multiple suppliers? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider(s)? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If critical fuel source(s) is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical fuel source(s) is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded:? ☐ 1-33% ☐ 34-66% ☐ 67- 99% ☐ 100% (Offline)

Critical Products – Fuels not including fuel for backup generators (e.g., diesel, gasoline, Aviation fuel)

Fuel for emergency electric generators is addressed in the Electric Dependencies section and should not be repeated in this section.

Natural gas for electric generation is addressed in Natural Gas Dependencies section and should not be repeated here. However, diesel fuel-fired electric generation plants would address diesel as its fuel for this section.

Please, do not fill in this section if fuels are not provided by an external provider.

Is there a contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of Fuels.

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If critical fuel source(s) is lost (without considering any backup or alternative source), how soon would the facility be severely impacted?

This question captures the impact of the worst case scenario, the fact that the facility loses access to critical fuel source(s) and is unable to use a backup or alternative source.

Once critical fuel source(s) is lost (without considering any backup or alternative source), what percentage of normal business functions would be lost or degraded?

This question captures the impact of the worst case scenario, the fact that the facility loses access to critical fuel source(s) and is unable to use a backup or alternative source.

Dependencies – Critical Products - Fuels	
Fuels not including fuel for backup generators (e.g., diesel, gasoline, Aviation fuel)	Are there external regulations/policies that mandate the facility shut down after loss of main fuels supply including alternate? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Is there an alternate (e.g., onsite storage) to the source of fuels? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No percentage: _____ What is the duration of this alternative _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) If there is onsite storage, what is the capacity?_____ Gallons Once critical fuel source(s) is lost (**and considering your backup or alternative mode**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)
Critical Products Fuel Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of fuels. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the fuel is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or testing requirements (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external sources of fuels. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external source of fuels is lost during 7 days, what time will be needed for full resumption of core operations when the external sources of fuels is restored.

What is the duration of this alternative?
If the alternative considered is a storage, please consider the duration of this storage without replenishing.

Dependencies – Critical Products - Fuels	
Byproducts/wastes (e.g., sulfur, garbage)	Does the facility use byproducts/wastes (e.g., sulfur, garbage) removal/disposal services for core operations? ☐ No ☐ Yes *List:* _____ What byproduct/waste is the most critical to core operations? _____ **For the most critical byproducts/wastes answer the following:** Is the most critical byproduct/waste removal service available from multiple suppliers? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider(s)? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If critical waste disposal service(s) is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical waste disposal service(s) is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded:? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Critical Products – Byproducts/wastes

If the facility has byproducts/wastes the disposal of which is a critical function to the continued operations of the facility, complete this section. For instance, the accumulation and storage of hazardous waste and medical waste are regulated and if offsite disposal options are not available, a facility must either stop processes that produce the waste or seek an exemption from the environmental regulatory body.

Please, do not fill in this section if byproducts/wastes are not removed by an external organization.

Contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of byproducts/wastes removal service.

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If critical waste disposal service(s) is lost (without considering any backup or alternative mode), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations):

This question captures the impact of the worst case scenario, the fact that the facility loses access to critical byproducts/wastes removal/disposal service(s) and is unable to use a backup or alternative source.

Once critical waste disposal service(s) is lost (without considering any backup or alternative mode), what percentage of normal business functions are lost or degraded:

This question captures the impact of the worst case scenario, the fact that the facility loses access to critical byproducts/wastes removal/disposal service(s) and is unable to use a backup or alternative source.

Dependencies – Critical Products – Byproducts/wastes	
Byproducts/wastes (e.g., sulfur, garbage)	Are there external regulations/policies that mandate the facility shut down after loss of waste removal service including alternate? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Is there an alternate (e.g., onsite storage) for byproducts/wastes disposal? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No percentage: _____ What is the duration of this alternative _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical waste disposal service(s) is lost (**and your backup or alternative mode is employed**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)
Critical Products Byproduct/Waste Briefing Notes: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of byproduct/waste disposal service. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

For example, a facility could be in the obligation, for a question of hygiene or security, to shut down if dangerous materials or garbage are not picked up. However, a delay could exist before the shutdown.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the byproducts/wastes disposal service is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or regulatory requirements (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external byproducts/wastes disposal service. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external byproducts/wastes disposal service is lost during 7 days, what time will be needed for full resumption of core operations when the external byproducts/wastes disposal service is restored.

What is the duration of this alternative?
If the alternative source is storage, consider the duration of this storage without replenishment.

Dependencies – Critical Products – Byproducts/wastes	
Raw Materials (e.g., metals, plastic, lumber)	Does the facility use Raw Materials critical for its core operations? ☐ No ☐ Yes *List:* _____ What raw material is the most critical to core operations? _____ **For the most critical raw materials answer the following:** Is the most critical raw material available from multiple suppliers? ☐ No ☐ Yes Is there a contingency/business continuity plan with provider(s)? ☐ No ☐ Yes *Explain*: _____ Does the facility participate in provider priority plan for restoration? ☐ No ☐ Yes *Explain*: _____ If critical raw materials source(s) is lost (**without considering any backup or alternative mode**), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical raw materials source(s) is lost (**without considering any backup or alternative mode**), what percentage of normal business functions are lost or degraded:? ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)

Critical Products – Raw Materials

Raw materials can be any critical products that the facility uses but does not manufacture onsite. This could include lumber, spark plugs, or other items but should not include materials covered in other categories (e.g., fuel, chemicals, packaging). **Critical elements such as steam distribution, chilled water distribution, livestock feeds, and medical supplies should be captured in this section.**

Please, do not fill in this section if raw materials are not provided by an external provider.

Contingency/business continuity plan with provider for restoration
The intent of this question is to define if specific service level agreements exist between the facility and the provider of raw materials.

Does the facility participate in a provider priority plan for restoration?
A priority plan is a list of facilities or types of facilities at which service will be restored before other types of facilities. For instance, most utilities will prioritize human health facilities such as hospitals, water treatment system assets, and nursing homes and restore service to them before other customers.

If the critical raw materials source(s) is lost (without considering any backup or alternative source), how soon would the facility be severely impacted (e.g., more than 50% reduction in facility operations)?
This question captures the impact of the worst case scenario, the fact that the facility loses access to critical raw materials source(s) and is unable to use a backup or alternative source.

Once critical raw materials source(s) is lost (without considering any backup or alternative mode), what percentage of normal business functions would be lost or degraded?
This question captures the impact of the worst case scenario, the fact that the facility loses access to critical raw materials source(s) and is unable to use a backup or alternative source.

Dependencies – Critical Products – Raw Materials	
Raw Materials (e.g., metals, plastic, lumber)	Are there external regulations/policies that mandate the facility shut down after loss of raw material supply including alternate? ☐ No ☐ Yes Describe: _____ After how long? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once service is restored, how long would it take before full resumption of operations? _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Describe: _____ Is there an alternate (e.g., onsite storage) for raw materials? ☐ No ☐ Yes Describe: _____ Can this alternative support full core operations? ☐ Yes ☐ No percentage: _____ What is the duration of this alternative _____ minutes (enter the number of minutes) OR _____ hours (enter the number of hours) OR _____ days (enter the number of days) Once critical raw materials source(s) is lost (**and considering your backup or alternative mode**), what percentage of normal business functions are lost or degraded: ☐ None ☐ 1-33% ☐ 34-66% ☐ 67-99% ☐ 100% (Offline)
Critical Products Raw Material Briefing Notes: _____	
Overall Critical Product Comments: _____	

External regulations/policies
The intent of this question is to determine if external regulations/policies mandate the facility shut down after loss of the main source of raw materials. The answer is YES if the facility has specific procedures defining that the facility must shut down. The answer is YES if the facility owner/operator determines that it would be too dangerous or expensive to operate on backup after a certain time. This question relates directly to the facility's tolerable level of degradation, i.e., the amount of degradation they can tolerate before losing their ability to maintain core functions safely and effectively.

Restoration time
The intent of this question is to determine the time needed for the facility to resume normal operations after the byproducts/wastes disposal service is restored. While in many cases the restoration time will be automatic/immediate, it is possible that a delay could occur due to the unique restoration requirements of certain processes or regulatory requirements (i.e., lag time). The restoration time can vary based on the duration of the interruption. Answer to this question should be based on the Maximum Acceptable Outage (MAO) defined when considering the loss of external byproducts/wastes disposal service. If the MAO has not been defined, consider a **maximum outage duration of 7 days**: if the external byproducts/wastes disposal service is lost during 7 days, what time will be needed for full resumption of core operations when the external byproducts/wastes disposal service is restored.

What is the duration of this alternative?
If the alternative source is storage, consider the duration of this storage without replenishment.

COMMENDABLES

PMI and RMI - Commendables	
Information Sharing	*Describe:* _____
Security Activity History and Background	*Describe:* _____
Parking - Delivery - Standoff	*Describe:* _____
Overall Commendables Comments: _____	

PMI - Commendables	
Security Management Profile	*Describe:* _____
Security Force Profile	*Describe:* _____
Perimeter Security	*Describe:* _____
Entry Controls	*Describe:* _____
Barriers	*Describe:* _____
Building Envelope	*Describe:* _____
Electronic Security Systems	*Describe:* _____
Illumination	*Describe:* _____
Overall Commendables Comments: _____	

RMI - Commendables	
First Preventers/Responders	*Describe:* _____
Natural Hazards	*Describe:* _____
Resilience Management profile	*Describe:* _____
Dependencies	
Electric Power:	*Describe:* _____
Natural Gas:	*Describe:* _____
Communications:	*Describe:* _____
Information Technology:	*Describe:* _____
Transportation:	*Describe:* _____
Critical Products:	*Describe:* _____
Water:	*Describe:* _____
Wastewater:	*Describe:* _____
Overall Commendables Comments: _____	

VULNERABILITIES AND OPTIONS FOR CONSIDERATION

PMI and RMI – Vulnerabilities and Options for Consideration		
Information Sharing	*Describe:* _____	*Describe:* _____
Security Activity History and Background	*Describe:* _____	*Describe:* _____
Parking - Delivery - Standoff	*Describe:* _____	*Describe:* _____
Overall Vulnerability Comments: _____		

PMI - Vulnerabilities and Options for Consideration		
Security Management Profile	*Describe:* _____	*Describe:* _____
Security Force Profile	*Describe:* _____	*Describe:* _____
Perimeter Security	*Describe:* _____	*Describe:* _____
Entry Controls	*Describe:* _____	*Describe:* _____
Barriers	*Describe:* _____	*Describe:* _____
Building Envelope	*Describe:* _____	*Describe:* _____
Electronic Security Systems	*Describe:* _____	*Describe:* _____
Illumination	*Describe:* _____	*Describe:* _____
Overall Vulnerability Comments: _____		

RMI - Vulnerabilities and Options for Consideration		
First Preventers/Responders	*Describe:* _____	*Describe:* _____
Natural Hazards	*Describe:* _____	*Describe:* _____
Resilience Management profile	*Describe:* _____	*Describe:* _____
Dependencies - Vulnerabilities and Options for Consideration		
Electric Power:	*Describe:* _____	*Describe:* _____
Natural Gas:	*Describe:* _____	*Describe:* _____
Water:	*Describe:* _____	*Describe:* _____
Wastewater:	*Describe:* _____	*Describe:* _____
Communications:	*Describe:* _____	*Describe:* _____
Information Technology:	*Describe:* _____	*Describe:* _____
Transportation:	*Describe:* _____	*Describe:* _____
Critical Products:	*Describe:* _____	*Describe:* _____
Overall Vulnerability Comments: _____		

POTENTIAL ADDITIONAL DHS PRODUCTS

Potential Additional DHS Products/Services to Discuss
Additional Assessments: ☐ BZPP ☐ Cyber/SCADA ☐ Dependencies/Interdependencies ☐ Threat ☐ Blast Effects ☐ Self-Assessment Tools Additional Information Available: ☐ Common Vulnerability, Potential Indicator, Protective Measure papers ☐ Background Package ☐ Grant information ☐ HSIN Access ☐ GETS Cards ☐ GIS Products ☐ Training Opportunities ☐ Exercises ☐ Tripwire ☐ Special Request Identify: _____ Miscellaneous: ☐ Coordination request ☐ DHS Private Sector Security Clearance Program (Facility) ☐ State-Homeland Security Clearance Program (Public-sector) ☐ Other: Identify: _____ Comments:
Overall Comments: _____

This page is intentionally left blank

Homeland Security