RAPID SURVEY

The Rapid Survey Tool Question Set on the following pages can be printed out and used as a type of “notebook” while conducting a survey.

This notebook is best printed dual sided, flip on long edge.

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.

When you have answered some of the security-related questions, but not all 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 Offline upload (with data check) is complete:

- You are required to **shred this notebook**.

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

This page is intentionally left blank

Security Management Profile

Does the facility have a written physical security plan?

A physical security plan is an important component of a facility's overall security management strategy; it provides written guidance for the implementation of physical security measures. It is distinct from other types of plans, such as emergency operations plans, and business continuity plans. Normally, physical security planning includes those things that involve security issues, such as active shooter, terrorism, hostage taking, or assassination.

Physical security is a critical element of an effective risk management strategy. Generally speaking, a well-developed security plan

- Explains the purpose of the plan
- Identifies those individuals who are responsible for execution of the plan and what their responsibilities are
- Identifies policies for the protection of specific assets, and
- Establishes access control measures.
- In addition, the plan has procedures for:
    - 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.
    - Exercising the plan: This section outlines how essential equipment or a process is tested, how employees and key personnel are trained and evaluated on the plan, and the regimen for exercising the plan.

Are personnel trained on the plan?

Physical security plan training is important because it increases an employee's safety awareness and contributes to a safer, more secure work environment. Physical security plan training can range from giving the employee a copy of the plan and asking them to read it, to instructor-led courses, instructional videos, and webinars, along with tests of the employee's level of understanding of the plan.

To the extent that the facility's personnel are not trained on the physical security plan, the plan, no matter how detailed it may be, will have no practical value. Thus, it is extremely important that, at a minimum, key personnel are trained on the plan, i.e., they are made familiar with the plan's procedures and know how to execute those procedures if and when the need arises.

Is the plan exercised at least once a year?

The purpose of this question is to determine when the facility's physical security plan is tested in some manner before an actual emergency occurs. Exercising the plan enables those responsible to more accurately assess the extent to which the plan's provisions can be implemented and how likely the plan will be effective in addressing an emergency should one arise.

Examples of exercises of the physical security plan include the following:

- Tabletop (practical or simulated) exercises: Tabletop exercises are designed to help a facility test its ability to respond to a hypothetical situation, such as a natural or man-made disaster, evaluate the ability of the facility's personnel to cooperate and work together, and test the facility's readiness to respond. Tabletop exercises can also include external responders.
- Functional (walk-through or specialized) exercises: A functional exercise simulates an emergency in a realistic manner, without moving people and equipment to an actual site. Its goal is to test or evaluate the capability of one or more of a physical security plan's functions in an event. A functional exercise is similar to a tabletop exercise except that the functional exercise requires more scripting, planning, and attention to detail. Functional exercises can also include external responders.
- Full scale (simulated or actual event) exercises: A full-scale exercise is as close to the real thing as possible. It is a lengthy exercise that takes place on location, using, to the extent possible, the equipment and personnel that would be called on in a real event. A full-scale exercise is designed to challenge the overall physical security plan in a highly realistic and stressful environment. Field-based action is a major difference between full-scale and functional exercises. A full-scale exercise can include external responders.

Does the facility have a written physical security plan?	○ Yes	○ No
Are personnel trained on the plan?	○ Yes	○ No
Is the plan exercised at least once a year?	○ Yes	○ No

Is there a manager/department in charge of security management?
As a rule, facilities that have developed a written physical security plan appoint someone to be in charge of security management. In particular, the manager is responsible for ensuring that relevant parties are aware of and familiar with the plan and that they know how to execute the plan if and when the need arises.

Does the facility have procedures for suspicious packages?
Suspicious packages procedures spell out the steps that should be taken when an employee encounters a package (letter or parcel) that raises safety concerns. Suspicious package procedures address items that might be encountered in mailrooms, as well as packages that might be found in or near a facility.

The list of procedures for addressing suspicious packages typically includes:

- Instructions on how the package in question should (or should not) be handled,
- Who should be notified, both internally and externally, when a suspicious package is discovered, and
- Evacuation instructions

In addition, numerous characteristics of a suspicious package have been identified. The list of characteristics includes:

- Rigid or bulky
- Lopsided or uneven
- Wrapped in string
- Badly written or misspelled labels
- Generic or incorrect titles
- Excessive postage
- No postage
- Foreign writing, postage, or return address
- Missing, nonsensical, or unknown return address
- Leaks, stains, powders, or protruding materials
- Ticking, vibration, or other sounds

Does the facility participate in any security working groups?
A working group refers to a group of individuals who are brought together temporarily until a stated goal or objective is achieved. A security working group typically involves people from different organizations with expertise in security-related matters. Of interest here is whether the facility is participating in any security-focused working groups at the federal, state, local or industry/private level.

Examples of security working groups include:

- Federal-level security working groups (e.g., InfraGard, Sector Coordinating Committee),
- State-level security working groups (e.g., Fusion Center),
- Local-level security working groups, and
- Private Sector /Industry security working groups.

Is there a manager/department in charge of security management?	○ Yes	○ No
Does the facility have procedures for suspicious packages?	○ Yes	○ No
Does the facility participate in any security working groups?	○ Yes	○ No

Are background checks conducted?
The intent of this question is to determine if there is a process for background checks on employees. Often background checks are a reasonable action to dissuade insider threats or to ensure effective hiring practices.

Background checks can range from rudimentary, e.g., examination of a person's resume' or searching the person's name on the Internet, to hiring a security firm to do an in-depth check on a person's background, including employment verification and work history; validation of references; education, certification and licenses background; credit history (including bankruptcy); military record; drug testing; and criminal record.

It is understood that there may be limitations to background checks in some states or for foreign contractors.

On all employees?
"YES" should be selected only if all the facility's employees are subjected to background checks. Note, however, that the term "employees" does not include contractors, vendors, or contract security personnel.

A contractor/vendor is defined as anyone who comes to the facility for the purposes of conducting work such as maintenance, construction, security, refill food or drink machines, deliver materials, or a host of other reasons. This category also includes contractors who are employed by the facility directly and may work alongside the regular employees of the facility; for example, a Company ABC employee who is contracted by Company XYZ and works at XYZ's Chicago office. This also includes a security force that is contracted, such as Wackenhut or Securitas, to provide various levels of security for a facility.

Are recurring background checks conducted?
Frequently, background checks are performed only when a person is initially considered for employment. Although a background check may show a clean record when an employee is hired, however, an employee's background may be altered in a significant way, e.g., the employee commits a crime while employed that does not immediately come to the employer's attention. Periodic checks are a way to identify such situations and provide increased protection to the workplace.

Are background checks conducted?	○ Yes	○ No
On all employees?	○ Yes	○ No
Are recurring background checks conducted?	○ Yes	○ No

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 part of a security force, in the R-IST definition those personnel are not considered security force personnel. The R-IST 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.

Is the security force armed?

The term "armed" simply refers to whether each member of the security force is equipped with a gun.

Is the security force on site?

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

To better understand the distinction between an onsite security force and a security force that would be considered "offsite", is an offsite security force is one whose personnel 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.

Does the facility have a security force?	○ Yes	○ No
Is the security force armed?	○ Yes	○ No
Is the security force on site?	○ Yes	○ No

Are there static posts?
Static posts are positions manned by stationary personnel for entry control, monitoring and/or protection. However, "YES" should only be selected if there is at least one static post that is staffed by security personnel. If there are static posts, but none are staffed by security personnel, then select "NO."

Static posts may be located at an entry/access control point, such as a gate or door, to control entry, but also could be located 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. Static posts also include personnel designated to monitor facility command and control centers. It does not, however, include positions that monitor video surveillance or an intrusion detection system.

What percentage of the facility is covered?
To calculate the percentage of facility coverage, determine the number of static posts that have been established by the facility and then determine how many of those static posts are staffed by security personnel. The percentage of coverage is then determined by dividing the number of static posts staffed by security personnel by the total number of static posts.

For example, 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.

For a public venue, calculate the percentage 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%).

Are there roving patrols?
Roving patrols consist of 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 static posts and roving patrols, especially if it is a public venue.

Are there static posts? ○ Yes ○ No

What percentage of the facility is covered?

○ 1 - 25%
○ 26 - 50%
○ 51 - 75%
○ 76 - 99%
○ 100%

Are there roving patrols? ○ Yes ○ No

What percentage of the facility is covered?

○ 1 - 25%
○ 26 - 50%
○ 51 - 75%
○ 76 - 99%
○ 100%

Physical Security Profile

Is 100% of the facility enclosed in fencing?
As it is used here, the term "fence" could be a wall or any structure or natural barrier that would prevent entry (e.g., cliff or solid building) to the facility in question.

In determining the percentage of the facility that is enclosed in fencing, the focus should be on the weakest area of the fence that protects the facility or entry to pertinent parts of the facility. For example, the facility may have an 8-foot chain link fence with a razor wire topper that covers 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 it would be concluded that less than 100% of the facility is enclosed in fencing.

That being said, it is important to consider whether a 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 the facility, then look for another weak section of fence. If no other weak sections of fence exist, it would be concluded that 100% of the facility is enclosed in fencing.

Additional examples in which less than 100% of the facility is enclosed in 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, however, is not fenced; thus, the bridge cannot be 100% fenced. It would also be unusual for a railroad, rail yard, bus route, or pipeline to have 100% fencing. On the other hand, if the facility is within a larger complex that is 100% fenced, then the facility has 100% fence coverage.

Is there a clear zone around the perimeter (an area that allows for clear sight of fence perimeter with no vegetation, objects or privacy slats)?
A clear zone refers to an area both outside and inside the fence that should be clear of vegetation and other places of concealment. A clear zone aids in the surveillance of the fence line and the identification of potential intruders or areas where the integrity of the fence has been compromised.

Does the facility use vehicle gates?
The purpose of this question is to determine whether the facility employs gates that restrict entry by various types of vehicles (e.g., cars, trucks, buses, motorcycle) to pertinent parts of the facility.

Does the facility use pedestrian gates?
The purpose of this question is to determine whether the facility employs gates that restrict entry by individuals on foot to pertinent parts of the facility.

Is 100% of the facility enclosed in fencing?	○ Yes	○ No
Is there a clear zone around the perimeter (an area that allows for clear sight of fence perimeter with no vegetation, objects or privacy slats)?	○ Yes	○ No
Does the facility use vehicle gates?	○ Yes	○ No
Does the facility use pedestrian gates?	○ Yes	○ No

Does the facility have ground floor windows (less than 18 feet from the ground)?
The purpose of this question is to determine whether the facility is vulnerable to the impact of a bomb explosion on glass (although it is understood that windows above the ground floor are also susceptible). If the facility is made of glass "walls" indicate that the building has windows. By definition, if a facility is not contained within a building, there are not windows and the question should be answered "NO."

Are there protective measures on the ground floor windows for the facility?
The focus should be on the weakest windows found in buildings that are the primary facilities. For example, although a facility may have impact resistant glass in most ground-floor windows, the building may have one or more windows with plain single pane glass. In this example, although the vast majority of the windows are excellent, the single pane glass window constitutes a vulnerability. Therefore, the single pane glass windows are the ones on which the question should focus and will be used for scoring purposes. The list of relevant protective measures includes: blast curtains, blast/safety film, bullet-proof glass, laminated glass, wire-reinforced glass, and thermally-tempered glass.

A description of each of the relevant protective measures follows:

- 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.
- 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

Does facility have an air handling system with an external air intake less than or equal to 10 feet from the ground with unrestricted access?
If the facility is an enclosed building, there is a good chance that there is an air handling system of some type. 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.

This question does not typically want to identify a small window air conditioner. Rather, the question is referring to the heating, ventilation, and air conditioning system within a facility.

Does the facility have ground floor windows (less than 18 feet from the ground)?	○ Yes	○ No
Are there protective measures on the ground floor windows for the facility?	○ Yes	○ No
Does facility have an air handling system with an external air intake less than or equal to 10 feet from the ground with unrestricted access?	○ Yes	○ No

Does the facility utilize video surveillance?
Video surveillance, which is also referred to as closed-circuit television (CCTV), uses one or more video cameras to transmit a signal to a specific location and a limited set of monitors. Video surveillance is typically employed in areas that may need monitoring such as banks, airports, and convenience stores.

There are two types of video surveillance:

- Digital camera, record, and display systems: Almost all systems put in place within the last 5 years are likely digital. If there is a DVR, there is a good chance the system is digital.
- Analog camera, record, and display systems: This is almost always an older system. If the record system is VCR tape, the system is analog.

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

Pan-Tilt-Zoom cameras allow one 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 degrees) without moving. Fixed cameras have a straight view that does not change.

Transmission media include

- Fiber cable: a cable made up of super-thin filaments of glass or other transparent materials that can carry beams of light.
- Wire line (twisted pair): a cable with multiple pairs of twisted insulated copper conductors in a single sheath.
- Coaxial: a cable transmission which may be base-band video or video-modulated radio frequency.
- Wireless: a microwave or IP network to send information with sufficient bandwidth.

Does a trained security staff monitor the video surveillance?
For the purposes of this question, the term “trained security staff” includes all staff trained in surveillance detection and how to identify suspicious activity. This question should be answered “YES” even if surveillance coverage is less than 24/7/365.

If monitoring is conducted by anyone other than trained staff, i.e., non-security personnel such as a receptionist, or there is no real-time monitoring of the video surveillance, the appropriate response in “NO.”

Does the facility utilize video surveillance?	○ Yes	○ No
Does a trained security staff monitor the video surveillance?	○ Yes	○ No

For each of the following groups, are controls in place that limit entry?
This question is concerned with whether entry to a facility by different groups of individuals is monitored or restricted. For each of the four groups listed, if no restrictions are in place, answer "NO."

Employees
An employee is defined as an individual who works for that particular facility. If you were to look at the individual's pay statement it would clearly state the person is employed directly by Company XYZ. The term "employee" does not include contractor/vendor regardless of how integrated the contractor is into the company. All facilities will have one or more employees there at some point in time and entry controls should always be completed for employees.

Visitors
A visitor is defined as an individual who 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 one or more employees at the facility. It is possible, yet 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.

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

Customer/Patron/Public
The term customer/patron/public is limited to any situation where the facility 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, because 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, because 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.

For each of the following groups, are controls in place that limit entry?

Employees	○ Yes	○ No
Visitors	○ Yes	○ No
Contractors/Vendors	○ Yes	○ No
Customer/Patron/Public	○ Yes	○ No

Can any vehicle be placed (legally or illegally) within 400 feet of the facility?
This question is concerned with the consequences of an explosion from a vehicle-borne improvised explosive device (VBIED) that has been placed close to a facility. If the only parking allowed is more than 400 feet from the facility, it can be assumed that a facility is better protected from the adverse effects of a VBIED.

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.
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.

Does the facility have one or more avenues of high speed 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 before the attack can be detected, deterred, or interdicted. If a facility has installed traffic calming, road redirection, berms, or jersey barriers such that a high speed avenue of approach is now mitigated, select "NO." (While the facility may have once had that vulnerability, it is mitigated and no longer exists because of specific actions the facility has taken to solve that vulnerability.)

The term “high speed avenue of approach” does not apply only to roads. For example, a high speed avenue of approach still exists if a facility is located near a fenced perimeter, and 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 the devices are placed in such a manner that the barriers can be avoided, are too far apart, or are lightweight plastic barrels or cones that will not impede vehicle travel.

Does the facility 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, 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, the high speed avenue of approach should not exist, i.e., the answer to the question: “Does the facility have one or more avenues of high speed approach?” is “NO.”

There are various types of barriers that can be used to mitigate a high speed avenue of approach. Examples include:

- 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. Jersey barriers 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.

- 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.

Does the facility use barriers to enforce standoff?
This refers to the situation in which the facility uses barriers to prevent vehicles from parking closer to the facility than the location of the barriers. The barriers in question 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.

Can any vehicle be placed (legally or illegally) within 400 feet of the facility?	○ Yes	○ No
Does the facility have one or more avenues of high speed approach?	○ Yes	○ No
Does the facility use barriers to mitigate a high-speed avenue of approach?	○ Yes	○ No
Does the facility use barriers to enforce standoff?	○ Yes	○ No

Is the illumination of fences, gates, and parking areas similar and uniform in type with overlapping light pattern coverage in most areas?

Is the illumination of building entrance and delivery areas similar and uniform in type with overlapping light pattern coverage in most areas?

"Uniformity" refers to a combination of type and coverage. An approximate determination of uniformity can be made by looking at the type of light and the spacing of the light fixtures. Type of illumination takes into consideration the type of bulb or light emitted. 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.

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. 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. Regardless of the area being evaluated, the focus should be on the weakest or most vulnerable area. If a facility does not have any fences, gates or parking then "YES" should be selected. "YES" is selected because the lack of illumination is not adversely affecting the facility's protective posture. The most common situation in which this condition applies will be waterside facilities.

It is also possible that an area has not been illuminated on purpose because a facility has determined that illuminating an area showcases or highlights a vulnerability. There may be lights at a given 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. Assuming all other areas satisfy the conditions for answering "YES," "YES" should be selected when this condition applies. This criterion should be used sparingly and only applies in isolated cases.

In situations where there is no illumination covering one or more areas, but a person would reasonably expect the area to have some illumination, "NO" should be selected. For example, it would be unusual to have a parking lot in a mall without some illumination. If there are 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 once again "NO." If there are multiple gates but only some of the gates are illuminated, then the interviewer must determine whether 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.

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.

Are illumination systems controlled by software applications?
A software application is a computer program that analyzes the information relevant to the operation of the illumination system, e.g., information collected by a motion detector, low light conditions. In this case, the software application processes the relevant information and then uses the results of the analysis to trigger the illumination system, e.g., cause lights to turn on, when conditions warrant.

Is the illumination of fences, gates, and parking areas similar and uniform in type with overlapping light pattern coverage in most areas?	○ Yes	○ No
Is the illumination of building entrance and delivery areas similar and uniform in type with overlapping light pattern coverage in most areas?	○ Yes	○ No
Are illumination systems controlled by software applications?	○ Yes	○ No

Does the facility utilize an interior intrusion detection method or application?
Interior intrusion detection systems (IDS) methods or applications are those that employ sensors 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 this question should be answered "NO" if that is the case. If the facility is not within a building, this question should be answered "NO."

Interior IDS systems utilize a range of sensors, including

- 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 Sensor

- Vibration Sensor – Detects the movement of the door.

- Glass Breakage Sensor, – Mounted directly on the glass, they are vibration sensors designed to generate an alarm when the frequencies more nearly associated with breaking glass are present.
- Conducting Tape – 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 – 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 – Ssimilar 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 Sensor

- Vibration Sensor – Detects 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 – 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 – A type of vibration sensor that uses mesh within a window that prevents glass from shattering and sets off the alarm.
- Magnetic Contact – 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.

Are the intrusion detection systems controlled by software applications?

A software application is a computer program that analyzes the information collected by the IDS. In this case, the software application processes the information collected by the IDS and then uses the results of the analysis to alert the appropriate individuals when suspicious activity is detected.

Does the facility utilize an interior intrusion detection method or application?	○ Yes	○ No
Are the intrusion detection systems controlled by software applications?	○ Yes	○ No

Does the facility have a written agreement with entities other than emergency responders?
This is different than a written agreement (e.g., an MOU or MOA) with emergency responders and may include Mutual Aid Agreements with neighboring facilities, contract chemical response companies, or private cleanup contractors.

Does the facility participate in security exercises or tabletops with outside agencies?
The intent of this question is to capture whether the facility, or one of its representatives, interacts with other people/organizations to share expertise and prepare to better respond to an emergency.

Does the facility have a written agreement with entities other than emergency responders?	○ Yes	○ No
Does the facility participate in security exercises or tabletops with outside agencies?	○ Yes	○ No

Resilience Management Profile

Is there a manager/department in charge of business continuity?

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

A business continuity manager/department conducts business impact analyses and risk assessments that include critical assets, functions (e.g., IT systems), building facilities, personnel, and supply chains. The business continuity manager 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.

Is there a manager/department in charge of business continuity?	○ Yes	○ No

Does the facility have a written business continuity plan?
The development and implementation of a business continuity plan (BCP) is vital to the overall resilience of any organization. A BCP helps prepare for any event that could impact critical operations or could have a negative impact on the company and/or facility. As such, a BCP contributes to reducing organizational consequences and enhancing an organization's ability to continue essential operations after an incident.

A well-conceived BCP will include the following elements:

- Identification of the essential functions of the organization, defining those that are critical to ensuring the minimal acceptable level of operation and prioritizing them from most to least critical;
- Identification of the potential hazards (e.g., natural, operational, and manmade, or equipment and supply chain failures) that could disrupt operations;
- Evaluation of the potential damage or loss to the facility/organization resulting from a disruption;
- Identification of strategies and activities to limit or control the potential consequences, extent, or severity of an incident that cannot be prevented; and
- Identification of response and recovery procedures for life safety, human resources, core operations, information technology, and other necessary organizational functions.

Does the plan include both physical and cyber assets?
Physical assets typically include buildings, machinery and equipment, inventory, and properties owned by the facility. Cyber assets include programmable electronic devices and communication networks including hardware, software, and data, for example, desktop, laptop, and mainframe computers, cloud providers, and server farms.

A more comprehensive list of cyber assets includes

- Control systems made up of devices or sets of devices that act to manage, command, or regulate the behavior of processes, devices, or other systems
- Data acquisition systems, i.e., collections of sensors and communication links that act to sample, collect, and provide data regarding the facility's systems to a centralized location for display, archiving, or further processing
- Networking equipment, including devices such as modems, switches, firewalls, routers and hubs
- Hardware platforms running virtual machines or virtual storage.

Are personnel trained on the plan?
The intent of this question is to capture whether facility personnel know the plan and its content (procedures), in addition to their role in the case of an incident. Experience indicates that exercises can validate training provided.

Following preparation of the BCP, it is necessary to develop a detailed implementation strategy that addresses training of key employees, access to the plan, and how the plan will be exercised. Although the planning process is certainly valuable, without appropriate implementation and use of the plan, much of the effort put into it may be lost. Once the plan is implemented, a documented maintenance and review strategy is critical. The strategy should include after-action reporting procedures following continuity exercises, as well as regular review and revision of the plan by senior leadership and key stakeholders (e.g., sole suppliers or utility providers).

Is the plan exercised at least once a year?
Exercising the BCP is the best way to prepare personnel to respond effectively to a business interruption. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events.

Exercises can include

- Tabletop (practical or simulated exercise), including external responders
- Functional (walk-through or specialized exercise), including external responders
- Full scale (simulated or actual event), including external responders

Does the facility have a written business continuity plan?	○ Yes	○ No
Does the plan include both physical and cyber assets?	○ Yes	○ No
Are personnel trained on the plan?	○ Yes	○ No
Is the plan exercised at least once a year?	○ Yes	○ No

Does the facility have a written 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. The intent of this question is to determine whether the facility has written 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 listed under "additional information," this question should be answered "YES" even if the facility does not have a plan specifically named "Emergency Operation Plan or Emergency Action Plan (EO/EAP)".

The purpose of an EO/EAP is to facilitate and organize employer and employee actions during workplace emergencies. Generally speaking, an EO/EAP addresses the time period immediately after an incident with the objective of returning critical facility operations to some minimum level. An EO/EAP would normally address things like weather, fire-related responses such as evacuation or shelter-in-place activities, and bomb threats or checklist type items. To illustrate, the U.S. Department of Labor's Occupation Health and Safety Administration (OSHA) regulations require that a facility's emergency action plan must include, at a minimum, the following:

- Procedures for reporting a fire or other emergency;
- Emergency evacuation procedures, including type of evacuation and exit route assignments;
- Procedures to be followed by employees who remain to operate critical plant operations before they evacuate;
- Procedures to account for all employees after evacuation;
- Procedures to be followed by employees performing rescue or medical duties; and
- The name or job title of every employee who may be contacted by employees who need more information about the plan or an explanation of their duties under the plan.

Well-developed EO/EAPs and proper employee training (such that employees understand their roles and responsibilities within the plan) should result in fewer and less severe employee injuries and less structural damage to the facility sustained during emergencies.

Does the plan include both physical and cyber assets?
Physical assets typically include buildings, machinery and equipment, inventory, and properties owned by the facility. Cyber assets include programmable electronic devices and communication networks including hardware, software, and data, for example, desktop, laptop, and mainframe computers, cloud providers, and server farms.

A more comprehensive list of cyber assets includes

- Control systems made up of devices or sets of devices that act to manage, command, or regulate the behavior of processes, devices, or other systems
- Data acquisition systems, i.e., collections of sensors and communication links that act to sample, collect, and provide data regarding the facility's systems to a centralized location for display, archiving, or further processing
- Networking equipment, including devices such as modems, switches, firewalls, routers and hubs
- Hardware platforms running virtual machines or virtual storage.

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. Experience indicates that exercises can validate training provided.

Following preparation of the emergency operation/emergency action plan, it is necessary to develop a detailed implementation strategy that addresses training of key employees, access to the plan, and how the plan will be exercised. Although the planning process is certainly valuable, without appropriate implementation and use of the plan, much of the effort put into it may be lost. Once the plan is implemented, a documented maintenance and review strategy is critical. The strategy should include after-action reporting procedures following exercises, as well as regular review and revision of the plan by senior leadership and key stakeholders (e.g., sole suppliers or utility providers).

Is the plan exercised at least once a year?
Exercising the emergency operation/emergency action plan is the best way to prepare personnel to respond effectively to an emergency. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events.

Exercises can include

- Drill (e.g., fire drill), including external responders
- Tabletop (practical or simulated exercise), including external responders
- Functional (walk-through or specialized exercise), including external responders
- Full scale (simulated or actual event), including external responders

Exercises should be evaluated to determine whether exercise objectives were met and to identify opportunities for program improvement.

Does the facility have a written Emergency Operation/Emergency Action Plan?	○ Yes	○ No
Does the plan include both physical and cyber assets?	○ Yes	○ No
Are personnel trained on the plan?	○ Yes	○ No
Is the plan exercised at least once a year?	○ Yes	○ No

Information Sharing

Does the facility receive threat information, security-related bulletins, advisories, and/or alerts from an external source?

Information that is received can include hazard analyses, intelligence, or information about specific incidents or events that may affect the facility.

A partial list of such sources includes the following:

- Federal
  - 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
- State/Local
  - Fusion Center
  - State CIP Coordinator
  - State Homeland Security Advisor
  - State/Local EMA
  - State/Local Law Enforcement
  - Industry Group
  - Public Health

Does the facility share threat and/or security-related information with outside organizations?

"Share" can mean "receive from," "provide to," or both. Information that is shared can include hazard analyses, intelligence, or information about specific incidents or events that may affect the facility. Facility EOCs can provide local and state EOCs with situational awareness of ongoing events and serve as a warning point.

Does the facility receive threat information, security-related bulletins, advisories, and/or alerts from an external source?	○ Yes	○ No
Does the facility share threat and/or security-related information with outside organizations?	○ Yes	○ No

Does the organization receive threat information, to include cyber-security-related bulletins, advisories, and/or alerts on cyber attacks and actors, from an external source?

It is essential that an organization fully understand what the cyber threats are in order to mitigate them. This is especially true where the threats are changing on a constant basis. Subscribing to external information sources allows the organization to keep abreast of all available threat research and reporting.

Examples of external sources of threat information covered by this question include:

- DHS entities
- FBI entities
- Vendors/industry (e.g. Industry ISACs)?
- State or local law enforcement department(s)
- Fusion Centers
- News sources

Specific DHS sources include:

- 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)

Does the organization receive vulnerability information, to include cyber-security-related bulletins, advisories, and/or alerts on technical vulnerabilities, from an external source?

It is essential that an organization fully understand what the cyber vulnerabilities are in order to mitigate them. This is especially true where the vulnerabilities are changing on a constant basis. Subscribing to external information sources allows the organization to keep abreast of all available vulnerability research and reporting as well as available patches, software modifications, and hardware fixes.

Does the organization share cyber-security information with outside organizations?

Sharing information benefits all organizations, including those within the sector and across all critical infrastructure in the U.S. It also benefits key suppliers and other groups that the organization may directly depend on. In addition, by sharing information, the organization opens itself to assistance in recovery and prevention from both public and private sources.

The types of information covered by this question include:

- Suspicious-activity reports
- Threat analysis
- Vulnerability analysis
- Subset of information reporting
- Confirmed incidents
- Status and configuration of security controls

Examples of the types of entities with which information might be shared include:

- Sector-specific information sharing and analysis center
- Sector-related associations/partnerships
- Federal or State-led partnerships (e.g., FBI InfraGard chapter(s))
- Fusion center(s)
- State or local law enforcement department(s)
- State or local IT office(s)

Does the organization receive threat information, to include cyber-security-related bulletins, advisories, and/or alerts on cyber attacks and actors, from an external source?	○ Yes	○ No
Does the organization receive vulnerability information, to include cyber-security-related bulletins, advisories, and/or alerts on technical vulnerabilities, from an external source?	○ Yes	○ No
Does the organization share cyber-security information with outside organizations?	○ Yes	○ No

Cyber Security Management

Is there a manager/department in charge of cyber security management?
For the purposes of this survey "cyber security management" includes the leadership roles and responsibilities (e.g., governance), physical documentation, lifecycle tracking, information sharing (e.g., threat information), accreditation, assessment, and audits.

Management responsibilities may be assigned to a single individual or a department so long as roles and responsibilities are slated to cyber security.

Is there an inventory of all critical cyber assets for this system?
It is critical that an organization understand and document all critical cyber assets. This inventory is the foundation for other security functions like access control, patching, auditing, configuration control, etc.

Cyber assets include programmable electronic devices and communication networks, including hardware, software, and data. Data and cabling are considered to exist within the framework of the cyber asset, and these are not separate cyber assets. A critical cyber asset inventory would include, at a minimum, the network addresses, machine names, purpose of each service, and asset owner responsible for each device.

A critical cyber asset inventory may also include every device with an IP address, including servers, desktops, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, VOIP, multi-homes addresses, virtual addresses, mobile phones, tablets, laptops, and other portable devices that store or process data.

Is there a documented security architecture that includes each of the identified critical cyber security assets?
For this survey, a documented critical cyber security asset security architecture should include all critical cyber security assets. The purpose of this question is to document the security architecture's approval for additional assets into the architecture document and how frequently it is reviewed and updated.

A documented system architecture could include the following: routers, switches, computers, servers, firewalls, VPNs, remote desktops, virtual machines, networks, etc.

Does the organization use system configuration monitoring procedures and/or tools that measure secure configuration elements and report configuration vulnerability information?
Configuration monitoring tools provide an automated view into the status of key security assets. For the purpose of this survey, examples of "system configuration monitoring procedures and/or tools" include: IBM Tivoli, IBM BigFix, Apache Subversion, & Perforce.

Does the organization have a documented and distributed cyber change management policy and supporting procedures?
Change management refers to the control procedures required to change the baseline configuration of a service. The baseline configuration is the set of specifications for a Service that has been formally reviewed and agreed on at a given point in time and can be changed only through formal change procedures. Configuration controls include controlling modifications to hardware, firmware, software,

and documentation to protect the information service against improper modifications prior to, during and after service implementation.

Does the organization employ measures to address system and data confidentiality, integrity, and availability requirements throughout their life cycle (design, procurement, installation, operation, and disposal)?

It is essential that an organization consider all security aspects through the full lifecycle of an application. These include confidentiality (keeping vital information out of the wrong hands), integrity (maintaining the accuracy and trustworthiness of the data), and availability (ensuring that the data and systems are running an availability as needed by the organization). Each of these aspects should be considered at the beginning of the design process and then should be reviewed during updates, additions, production implementation and finally, system retirement.

Is there a manager/department in charge of cyber security management?	○ Yes	○ No
Is there an inventory of all critical cyber assets for this system?	○ Yes	○ No
Is there a documented security architecture that includes each of the identified critical cyber security assets?	○ Yes	○ No
Does the organization use system configuration monitoring procedures and/or tools that measure secure configuration elements and report configuration vulnerability information?	○ Yes	○ No
Does the organization have a documented and distributed cyber change management policy and supporting procedures?	○ Yes	○ No
Does the organization employ measures to address system and data confidentiality, integrity, and availability requirements throughout their life cycle (design, procurement, installation, operation, and disposal)?	○ Yes	○ No

Does your organization implement at least one cyber-security standard(s) of practice (e.g., NIST SP800 series, NERC CIP, HIPAA, ISO/IEC 27000 series, etc.)?
Examples of additional standards covered by this question include:

- ISO/IEC 27000 Series
- CObit
- ITIL
- HITRUST
- ISF Standard of Good Practice (SOGP)
- FIPS 199
- NIST Cyber Security Framework

Is there a Cyber Security Plan covering the critical cyber security assets?
The answer to this question is "YES" if the facility has documentation that addresses cyber security or cyber service continuity. Cyber service continuity involves continuity of operations, business continuity, cyber disaster recovery, etc. These plans may exist separately or be included in the organization's overall plans but should address cyber specifically.

Organizations must develop, document, update, and implement security plans for organizational information services that describe the security controls to be in place and the rules of behavior for individuals accessing the information services.

Are personnel trained on the plan?
Having a cyber security plan is ineffective if it remains on a shelf. It is necessary to ensure that personnel are trained on the elements found in the plan.

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

Is the plan exercised at least once a year?
Exercising the cyber security plan is the best way to prepare personnel to respond effectively to an emergency. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events.

Does the organization conduct cyber security exercises?
Cyber security exercises provide real-world experience with security problems and cover topics including

- Cyber awareness
- Service testing
- Continuity planning
- Disaster recovery
- Incident preparedness
- Threat and incident coordination
- Partner readiness

Types of exercises that can be conducted include the following:

- Tabletop without external participants (practical or simulated exercise)
- Tabletop with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers)
- Functional without external participants (specialized exercise)
- Functional with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers)
- Full scale without external participants (simulated or actual event)
- Full scale with external participants (e.g., vendors, cyber contractors, regulatory agencies, or CIP providers)

For the purposes of this survey, tabletop, functional, and full scale exercises are distinguished from one another as follows:

- Tabletop: practical or simulated exercises are typically talked about but not executed in production.
- Functional: specialized exercise typically in a specific area that can be an isolated event.
- Full scale: simulated or actual event typically consuming the entire organization to practice.

Does your organization implement at least one cyber-security standard(s) of practice (e.g., NIST SP800 series, NERC CIP, HIPAA, ISO/IEC 27000 series, etc.)?	○ Yes	○ No
Is there a Cyber Security Plan covering the critical cyber security assets?	○ Yes	○ No
Are personnel trained on the plan?	○ Yes	○ No
Is the plan exercised at least once a year?	○ Yes	○ No
Does the organization conduct cyber security exercises?	○ Yes	○ No

Cyber Security Forces

Are the following positions formalized within your organization?

Cyber Security Incident Response Team Lead/Incident Commander

Has an individual in the organization been formally assigned the task of leading the facility's Security Incident Response Team (SIRT)? (This assumes a SIRT exists.)

The persons(s) recognizes that they have been assigned this role. Others in the organization do as well.

Security Operations Personnel (i.e., Security Administrators, Security Analysts)

Has the facility assigned one or more individuals to act as a cyber security administrator/cyber analyst?

Security Architect

A security architect's responsibilities often include the following:

- Ensuring the design, implementation, and security of applications, services, and infrastructure are up to date.
- Incorporating security into infrastructure and application design processes.
- Implementation and maintenance of information security controls.
- Network and application security/monitoring.
- Vulnerability scanning and remediation.
- Risk analysis.
- Reporting, and incident response.

Do cyber security personnel involved in day-to-day operations receive cyber training?

Cyber security training has become policy in most organizations but the standards used are different among each organization.

Examples of cyber training programs include:

- Industry-recognized certification
- Formal training from training organizations/vendors
- In-house/informal
- Video
- Web-based
- OJT (on-the-job training)

Are the following positions formalized within your organization?	○ Yes	○ No
Cyber Security Incident Response Team Lead/Incident Commander	○ Yes	○ No
Security Operations Personnel (i.e., Security Administrators, Security Analysts)	○ Yes	○ No
Security Architect	○ Yes	○ No
Do cyber security personnel involved in day-to-day operations receive cyber training?	○ Yes	○ No

Cyber Security Controls

Has the organization established a process for identity proofing and authentication to limit access to the critical cyber systems to only authorized persons?

Identity proofing refers to the process of determining and verifying that an individual is who he/she claims to be. Identity verification typically relies on some sort of identification, such as a physical card, biometric data, or RSA token, combined with a user name and password. Authentication goes beyond verification by requiring the individual to provide information typically know only to the individual in question, such as his/her favorite hobby, or name of the high school he/she attended.

Examples of types of identity proofing include the following:

- Risk-based: a non-static authentication system that takes into account the profile of a user requesting access to a system. An example is asking additional security questions if they login from a different computer or IP address.
- Controls-based: an approach that restricts system access to authorized users. This means that users have to authenticate based on their roles and they are only deemed their privileges based on what they need.
- Best-practices: is an example of authentication such as two-step verification. Using RSA keys and Cryptocards are examples of second steps of verification.

Does the organization practice the concept of least privileges (i.e., users are only granted access to the information, file, and applications required to fulfill their roles and responsibilities)?

An example of least privilege would be allowing a data entry clerk access to the data entry forms, but denying access to information such as projected revenues or employee payroll data.

This also applies to typical users of computer workstations who are not given administrator rights to their computers. This protects the computers and networks from malware that might use the advanced rights to do damage to networks, or the computer itself, when those rights aren't needed for daily activities.

Does the organization allow remote access to critical cyber services/assets?

Remote access allows connectivity to the internal network from the outside. User controls can include only allowing designated users to connect remotely, use of secure tokens, implementing virtual private networks (VPNs), changing passwords on remote devices, etc.

Examples of measures a facility can employ to control remote access to its cyber services include:

- Terms-of-use policies regarding user responsibilities and expected behavior
- Terms-of-use policies regarding service usage
- Terms-of-use policies regarding allowed and/or prohibited activities
- Access allowed only when needed, requested and authorized but disabled otherwise
- Remote-client filtering
- Multi-factor authentication
- Mandatory communications encryption
- Multiple session controls
- Session monitoring
- Session timeout

Has the organization established a process for identity proofing and authentication to limit access to the critical cyber systems to only authorized persons?	○ Yes	○ No
Does the organization practice the concept of least privileges (i.e., users are only granted access to the information, file, and applications required to fulfill their roles and responsibilities)?	○ Yes	○ No
Does the organization allow remote access to critical cyber services/assets?	○ Yes	○ No

Which of the following cyber security measures does the organization employ for monitoring of networks related to the critical cyber system?

Near-real-time monitoring for:

- Malicious code
  - Malicious code refers to successful installation of software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system, service, or application.
- Unauthorized access
  - As the name implies, unauthorized access refers to the situation in which a person or cyber system that has not been authorized or granted permission to do so gains access to the network.
- Intrusion detection
  - A cyber or network intrusion detection system monitors activities on a system or network in an effort to identify violations of established policies or activities of a malicious nature.
  - An intrusion detection system and a firewall are not the same thing.

Does the organization maintain security and event logs?

For purposes of this survey, event logging refers to log retention of services such as networks, endpoints, applications, etc. Event logging might entail recording application events (e.g., events logged by programs), security events (e.g., valid and invalid logon attempts), and system events (e.g., failure of a driver to load during start up).

Does the organization provide training on cyber security for critical cyber systems users?

Training on cyber security can cover a variety of topics, including:

- General review of organization's cyber policies
- Review of organization's cyber security policies
- User roles and responsibilities
- Password procedures
- Acceptable usage practices
- Identification and reporting of incidents and suspicious activities
- Cyber security situational awareness and best practices
- Cyber security threats, trends and attacks

Which of the following cyber security measures does the organization employ for monitoring of networks related to the critical cyber system? Near-real-time monitoring for:		
Malicious code	○ Yes	○ No
Unauthorized access	○ Yes	○ No
Intrusion detection	○ Yes	○ No
Does the organization maintain security and event logs?	○ Yes	○ No
Does the organization provide training on cyber security for critical cyber systems users?	○ Yes	○ No

Incident Response

Does the organization have predefined plans for responding to cyber security incidents?
Predefined plans for responding to cyber security incidents can include both a defined incident response plan for handling cyber incidents, and defined incident response procedures for handling cyber incidents.

A defined incident response plan can include

- Documented procedures, security violations and conditions, and assigned roles for cyber security incident response, or
- Assigned roles for cyber security incident response but no documented procedures

Defined incident response procedures for handling cyber incidents can include

- Planned procedures for network containment
- Planned procedures for malware containment(s) and boxing
- Planned procedures to rate limit in response to a Distributed Denial of Service attack
- Planned procedures to respond to an unauthorized access to sensitive information

Should your site become inoperable, do you have access to an alternative location?
The intent of this question is to ascertain whether the facility's core functions can be shifted to another location under the facility's control. 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.

Examples include the following:

- Assume a facility's data control center can operate from a location in another city; that is an alternative site.
- If a sports team can play in another stadium (e.g., the Bears played at the University of Illinois while their stadium (Soldier Field) was being modified), that is another example of an alternate site.
- Assume a shopping mall or a hotel has been severely damaged by a tornado. The fact that people can shop at an alternate mall is not an alternate site for the mall being assessed. The fact that there are other hotels in the area is not an alternate site for the damaged hotel.
- 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.
- Facilities such as manufacturing plants, hospitals, hotels, malls, bridges, tunnels, stadiums, arenas, racetracks, casinos, most general office buildings, and other similar types of facilities rarely have an alternate site.
- Data centers, government agencies/functions, banking, and communication facilities often have an alternate. Consider, for example, a redundant data center where data is backed up but operating terminals would have to be programmed/updated (e.g., cold site), or an operational control center at a corporate sister plant where operators can instantly log in as if they were located at the original location (e.g., hot site).

Does the organization have predefined plans for responding to cyber security incidents?	○ Yes	○ No
Should your site become inoperable, do you have access to an alternative location?	○ Yes	○ No

Dependencies

Cyber

Is the facility's core function dependent on data processing systems (mainframes, cloud providers, server farms, etc.)?
The purpose of this question is to determine whether the facility could complete its core function if internal data processing systems became unavailable. Core functions are those actions a facility must complete to achieve its mission.

For example, statistical analysis is a core function of a financial consulting firm. If the analysis is conducted in-house, then the firm's core function is dependent on internal data-processing systems.

Where is the location of the primary data processing systems and services?
The location of the primary data processing systems and services has implications for the vulnerability of those systems and services.

Are your data processing and cyber security functions managed by a third-party service provider, vendor or contractor?
Some facilities hire an external third party to manage/monitor their data processing functions 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.

In addition to management/monitoring of data processing and cyber security functions, 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.

Does the organization have alternative or backup storage capabilities that can be used in case of loss of the primary storage?
This question captures if the facility has procedures for data backup and the storage of those data. Alternative or backup storage capabilities guard against a disaster, e.g., fire, that could destroy the primary storage component and the data stored there. For example, a hospital might store electronic medical records at another location for later restoration of the original database/system.

If the primary mode of communication service is lost, is there a backup mode of communication?
Backup communications should be a different mode than the primary mode. For instance, if the facility's primary mode is 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.

Is the facility's core function dependent on data processing systems (mainframes, cloud providers, server farms, etc.)?	○ Yes	○ No
Where is the location of the primary data processing systems and services?		
Within the boundaries of the physical facility (on-site)?	○ Yes	○ No
At a data center located away from the facility (off-site data center, cloud service provider, etc.) Name Address City State ZIP Latitude Longitude	○ Yes	○ No
Are your data processing and cyber security functions managed by a third-party service provider, vendor or contractor?	○ Yes	○ No
Is data storage required for the critical cyber system?	○ Yes	○ No
Does the organization have alternative or backup storage capabilities that can be used in case of loss of the primary storage?	○ Yes	○ No
If the primary mode of communication service is lost, is there a backup mode of communication?	○ Yes	○ No

Electric

What is the facility's source of electrical power?
The purpose of this question is to determine whether the facility depends primarily on external or internal sources of electric power and to assist in the identification of systems and assets that are linked to or dependent on a damaged or compromised system or asset.

Does the facility possess and maintain a backup generator(s) capable of running mission critical services for 72 hours?
The intent of this question is to capture alternates and backups (backup generator and uninterrupted power system) in place in the facility that can provide electric power in case of loss of the primary source of electric power.

An uninterruptible power supply or uninterruptible power source (UPS) 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 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 includes both central and stand-alone devices. This difference is not critical. However, central UPS provides a more integrated solution. Specific examples include

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

Who is the facility's provider of electrical power? Name		
What is the primary substation that the facility is dependent upon? Name Address City State ZIP Latitude Longitude		
Is there a secondary or alternate substation for this facility? Name Address City State ZIP Latitude Longitude	○ Yes	○ No
Does the facility possess and maintain a backup generator(s) capable of running mission critical services for 72 hours?	○ Yes	○ No

Natural Gas

Is the facility's core function dependent on access to natural gas?
If the facility requires natural gas to complete its core functions the appropriate response to this question is "YES."

What is the delivery mechanism for the gas supply?
Virtually all natural gas is delivered via pipeline, while propane and CNG are usually delivered via truck.

Emerging technologies might prove cost effective for the delivery of smaller quantities of natural gas via truck. In almost all instances, however, natural gas is currently delivered via pipelines. Propane, because of its chemical make-up, is much easier to store in liquid form and is therefore much easier to deliver via truck.

Is the facility's core function dependent on access to natural gas?	○ Yes	○ No
Who is the facility's provider of natural gas?		
Name		
What is the facility's primary source of natural gas?		
Name		
Address		
City		
State		
ZIP		
Latitude		
Longitude		
Is there a secondary source of natural gas?	○ Yes	○ No
Name		
Address		
City		
State		
ZIP		
Latitude		
Longitude		
What is the delivery mechanism for the gas supply?		
Pipeline	○ Yes	○ No
Truck	○ Yes	○ No

Water

What is the source of the facility's water supply?

The purpose of this question is to determine whether the facility is dependent on an external source, e.g., the local water company, for its water supply.

If the source of the facility's water supply is external, the full name of the source is sufficient. If instead, the facility has an onsite source of water, the type of source, i.e., surface water or onsite wells, should be indicated.

Who is the facility's provider of water? Name		
What is the facility's primary source of water? Name Address City State ZIP Latitude Longitude		
Is there a secondary source of water? Name Address City State ZIP Latitude Longitude	○ Yes	○ No
Does the facility maintain onsite water storage capacity capable of sustaining operations?	○ Yes	○ No

Wastewater

Is the facility's core function dependent on continuous access to wastewater discharge services?
If the facility does not use an external wastewater discharge service (all wastewater is treated internally), please check "NO" and go to the next question.

In order to be dependent only on an internal 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, the appropriate response to this question is "YES" because the facility cannot operate upon loss of the wastewater service provider. It may be that domestic sewage is discharged to the local or regional wastewater authority, while industrial wastewater is treated onsite and discharged directly to a water body. Few facilities will have onsite domestic sewage treatment and discharge.

Is the facility's core function dependent on continuous access to wastewater discharge services?	○ Yes	○ No
Who is the facility's provider of wastewater discharge services?		
Name		
What is the facility's primary source of wastewater discharge services?		
Name		
Address		
City		
State		
ZIP		
Latitude		
Longitude		
Is there a secondary source of wastewater discharge services?	○ Yes	○ No
Name		
Address		
City		
State		
ZIP		
Latitude		
Longitude		

Communications

Is the facility's core function dependent on continuous access to communications infrastructure (e.g., wired phone, wired data, cell phone, etc.)?

If the facility does not receive any communications service from an external source, the appropriate response to this question is "NO."

Communication modes covered here include the following:

- 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.
- 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).
- 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).

Is the facility's core function dependent on continuous access to communications infrastructure (e.g., wired phone, wired data, cell phone, etc.)?	○ Yes	○ No

Name
Address
City
State
ZIP
Latitude
Longitude

Transportation

Is the facility's core function dependent on access to roadways, bridges, tunnels and highway infrastructure?

A dependency exists if the facility's core function could not be achieved because it was denied access to one or more of the infrastructures listed. In addition, if access to the facility is limited to a single road, bridge, tunnel, or highway, the appropriate response is "YES."

The following examples illustrate how to select the appropriate response to this question:

- If multiple public road routes or highways are available to reach the facility, the facility is not dependent on a single road.
- In rural areas, a long private-access road or single highway could create a dependency on the road mode of transportation; such a dependency on the road mode of transportation could be for commuting personnel, as well as delivery or shipment of products or wastes.
- Where access to the facility is limited to a single bridge or tunnel, the loss of which would isolate the facility, a dependency exists. (In urban areas, this would be rare.)

What are the key structures?

Please provide a full description/name of each structure, e.g., U.S. Highway 45, the Bong Bridge.

How long can the facility operate if these structures are compromised?

Please answer this question in hours or days.

Is the facility's core function dependent on access to any of the following transportation systems?

For each of the transportation systems listed, a dependency exists if the facility's core function could not be achieved because it was denied access to that system. In such cases, the appropriate response is "YES."

A dependency on a mode of transportation is identified as a single point of failure in the transportation system that would severely impact the operability of the facility. For example, if there are multiple public road routes to reach the facility, the facility is not dependent on a single road, so select NO for Shipping. Facilities that would be dependent on the shipping transportation system would be those where access is limited to a single route, the loss of which would isolate the facility. In urban areas, this would be rare.

This logic applies to all transportation modes. Occasionally, but rarely, a facility is dependent on 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. Assume 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.

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.

Is the facility's core function dependent on access to roadways, bridges, tunnels and highway infrastructure?	○ Yes	○ No
What are the key structures?		
How long can the facility operate if these structures are compromised?		
Is the facility's core function dependent on access to any of the following transportation systems?		
Rail	○ Yes	○ No
Air	○ Yes	○ No
Shipping	○ Yes	○ No
Waterways	○ Yes	○ No
Pipeline	○ Yes	○ No

Critical Products

Is the facility's core function dependent on access to chemicals and/or fuels?
The purpose of this question and the one that follows is to identify chemicals (e.g., nitrogen, hydrogen, chlorine) and/or fuels (e.g., diesel, gasoline, aviation fuel) the facility uses to achieve its core function.

What are the names of the chemical and/or fuels providers?
For Critical Products in each category, list only those that are absolutely necessary for the functioning of the facility.

Is the facility's core function dependent on byproduct and waste removal?
The purpose of this question to identify byproducts/wastes the disposal of which is a critical function to the continued operations of the facility.

For example, the accumulation and storage of hazardous waste and medical waste are regulated. 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."
Is the facility's core function dependent on reliable access to raw materials such as metals, plastics, rubber, lumber, etc.? "The purpose of this question is to identify raw materials (e.g., metals, plastics, rubber, lumber) the facility uses to achieve its core function.

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.

Is the facility's core function dependent on access to chemicals and/or fuels?	○ Yes	○ No
What are the names of the chemical and/or fuels providers?		
In the event of a disruption affecting your suppliers, do you have contracts with alternate suppliers?	○ Yes	○ No
Is the facility's core function dependent on byproduct and waste removal?	○ Yes	○ No
Is the facility's core function dependent on reliable access to raw materials such as metals, plastics, rubber, lumber, etc.?	○ Yes	○ No

General

If you are a supplier of critical goods or services to other entities please list them below.
The purpose of this question is to identify downstream dependencies.

If your facility experiences an unplanned service interruption, what are the impacts or consequences for your customers, the public, or other suppliers in the subsector/segment?
Some facilities may have backup plans for providing customers with goods or services through other contracts (e.g., a hospital may have a plan for transferring patients to other nearby facilities in the event of a business interruption; a chlorine repackager may have a standing contract with another sister company or even a competitor to provide chlorine to an essential customer).

If you are a supplier of critical goods or services to other entities please list them below.

If your facility experiences an unplanned service interruption, what are the impacts or consequences for your customers, the public, or other suppliers in the subsector/segment?

- ○ Loss of operations or serviced
- ○ Significant impact
- ○ No impact
- ○ Minor impact

Consequence

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, 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, only two US manufacturers produce 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. Few of these in the Nation have a large market share.

Is the facility a lifeline critical infrastructure (e.g., a utility provider/asset)?	○ Yes	○ No
Can other competitors or similar sister companies/facilities provide the product or service without major price impacts or delivery delays?	○ Yes	○ No

What is the maximum facility population at any one time (include special events, employees, contractors and visitors)?
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 off-site 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 on site that could be weaponized or stolen thus making that facility more likely to be targeted or may cause harm through accidental release.

What is the 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)?
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 off-site 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 off site 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.

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?
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). This will probably only be caused by a chemical or radiological release or similar event.

What is the maximum facility population at any one time (include special events, employees, contractors and visitors)?		
Is the facility considered a Chemical, Biological, Radiological, Nuclear, or Explosive facility?	○ Yes	○ No
What is the 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)?		
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?	○ Yes	○ No

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.

What is the asset replacement value?
Asset replacement costs apply to site equipment, units, or other on-site 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 that yields the highest damage should be used as the basis for the estimate.

What is the business interruption cost?
Business interruption costs include the total loss of sales or income for a 12 month period.

Is the facility part of a designated system (e.g., electric grid, pipeline, railroad, or mass transit system)?

What is the asset replacement value?

- ○ Less than $5,000,000
- ○ $ 5,000,001 to 20,000,000
- ○ $ 20,000,001 to 100,000,000
- ○ $ 100,000,001 to 500,000,000
- ○ $ 500,000,001 or greater

What is the business interruption cost?

- ○ Less than $10,000,000
- ○ $ 10,000,001 to 100,000,000
- ○ $ 100,000,001 to 500,000,000
- ○ $ 500,000,001 to 1,000,000,000

$ 1,000,000,001 or greater

This page is intentionally left blank

Threat Identification

Natural Hazards

- ☐ Avalanche
- ☐ Animal Disease Outbreak
- ☐ Drought
- ☐ Earthquake
- ☐ Flood
- ☐ Hurricane
- ☐ Landslide
- ☐ Pandemic
- ☐ Tornado
- ☐ Tsunami
- ☐ Volcanic Eruption
- ☐ Wildfire
- ☐ Winter Storm
- ☐ Other
  Please specify:

Technological (Accident)

- ☐ Airplane Crash
- ☐ Dam Failure
- ☐ Levee Failure
- ☐ Mine Accident
- ☐ Hazardous Materials Release
- ☐ Power Failure
- ☐ Radiological Release
- ☐ Train Derailment
- ☐ Urban Conflagration
- ☐ Other
  Please specify:

Human-Caused (Intentional)

- ☐ Biological Attack
- ☐ Chemical Attack
- ☐ Cyber Incident
- ☐ Explosives Attack
- ☐ Radiological Attack
- ☐ Sabotage
- ☐ School and Workplace Violence
- ☐ Other
  Please specify:

Cyber (Intentional

- ☐ Access via Wireless, Mobile, and Personal Devices
- ☐ Cloud Security
- ☐ Cyber Crime/Blackmail
- ☐ Data Breach/Loss
- ☐ Intellectual Property Theft/Corp Espionage
- ☐ Malware
- ☐ Distributed Denial of Service (DDOS)
- ☐ Code Injection
- ☐ Exploit Kits
- ☐ Social Media
- ☐ Targeted Cyber Attacks
- ☐ Other
  Please specify:

This page is intentionally left blank


U.S. DEPARTMENT OF HOMELAND SECURITY