FACILITY SECURITY SURVEY

Purpose: The facility survey tool has been designed for any private business to conduct an impartial and holistic review of their basic security posture. Due to the very nature and specificity of the questions, business owners may learn and adapt several security improvements for their applicable places of business. The survey is not regulatory in nature and should be treated as a protected document. The main goal is to focus on identifying vulnerabilities that can be mitigated at the least or totally corrected, depending upon the resources required and available. It is recommended to establish designated times throughout the year to complete the security survey to ensure that it is an ongoing improvement process; which can include adding additional questions as needed by the business.

Directions: Answer each question as you proceed down through the survey tool and total the number of "Yes" and "No" responses for each section. If you believe a question can be answered either way because your business possesses a portion of the question at hand, mark "No" regardless and review issue to see if it is possible to fully adopt the specific security measure in the future. You can analyze section by section as you review responses and discover vulnerabilities that can be corrected or mitigated.

Questions: If you have specific questions about your facility self-assessment, please reach out to your Department of Homeland Security Protective Security Advisor (PSA) (https://www.dhs.gov/protective-security-advisors) or the Ohio Homeland Security Infrastructure Protection Unit (https://homelandsecurity.ohio.gov/contacts.stm).

Appendix A

Facility Self-Assessment			
Building Identification and Access			
	Yes	*No*	*Options for Consideration for all Responses, as applicable*
1. Is the facility visible from the street during both the day and night so that police/security patrols can conduct external security checks?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
2. Are entry points to the facility/business supervised?			*Post security guards at entrances to facilitate access control procedures such as credential checks and searches on special event days.*
3. Do all employees, visitors, and vendors wear identification credential while on premises?			*Issue photo ID badges to all employees. Implement a process for badge verification before employees gain access to the facility. Collect employee badges from terminated personnel.*
4. Are visitors allowed entry to the building by appointment only, and do they have to report to a reception area before entry?			*DHS, 2011, Industry Protective Measures Report – Access Control Systems, p. 22.*
5. Are visitors escorted to and from their destination?			*Escort visitors as necessary, either at all times or only in sensitive/critical areas.*
6. Are visitors asked to provide proof of identification?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
7. Are visitors asked to sign in (preferably done by employee) when they enter the building?			*Fennelly, L., 2013, 2009, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.* *Skinner, Bradd M. C-TPAT Best Practices Catalog*

			Addendum., p. 12.
8. Are visitors provided with visitor's passes?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
9. Are passes designed to look different from employee identification?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
10. Are there external and internal signage to guide visitors?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
11. Are visitor passes collected from visitors when they leave the building?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
12. Do passes have an expiration date on them?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 261.*
13. Are visitors/customers prevented from accessing unauthorized areas such as utility rooms and sensitive areas?			*Escort visitors as necessary, either at all times or only in sensitive/critical areas.*
14. Do employees challenge or offer to assist people not wearing a visitor's pass or identification credential?			*Establish a policy for employees to approach unknown individuals around or in the facility.*
15. Are all incoming deliveries inspected before being delivered to the designated recipient?			*Consider inspecting all deliveries and packages prior to entering the facility.*
16. Are mail/package handling procedures posted in a conspicuous location?			*Implement U.S. Postal Service mail center security procedures to assess, prevent, and respond to threats such as suspicious letters and packages; bomb threats; and chemical, biological, or radiological contamination; Prominently display informational materials on suspicious package indicators in the mailroom.*
Column Total	(__ out of 16)	(__ out of 16)	

Fences and Gates			
	Yes	***No***	***Options for Consideration for all responses, as applicable***
1. Does the site have perimeter fencing that is free of visual obstructions (such as brush, bushes, containers, etc.) and clearly delineates the premises boundary?			*Establish clear zones on both sides of the fence to provide an unobstructed view to enhance detection and assessment. The dimensions of clears zones may vary depending on the asset being protected and level of protection required. Provide as much open space as possible between the fence and the facility.*
2. Are the fences constructed at a height to limit access? (six to eight feet high fences provide theft security.)			*Consult UFC 4-022-03, Security Fences and Gates, available at http://www.wbdg.org/ccb/DOD/UFC/ufc_4_022_03.pdf , for more information.*
3. Are gates in good working order and able to be secured by a locking device?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 112-113, p. 270; Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 47, p. 180, p. 263-265.*
4. Are security measures on gates sufficient to prevent forced entry?			*Integrate other security systems, including sensors, cameras, or other intrusion detection devices, at gates, as appropriate.*
5. Are there appropriate warning signs displayed around the perimeter of the premises?			*Post visible, well-placed warning signs on the gate. Signs may act as a deterrent and/or provide safety information for unauthorized personnel. In areas where two or more languages are commonly spoken, the warning signs must use both (or more) languages.*
Column Total	(__ out of	(__ out of	

	5)	5)	
Doors and Windows			
	Yes	***No***	***Options for Consideration for all responses, as applicable***
1. Are door and window frames made of solid materials?			*Conduct an assessment to determine additional appropriate, feasible mitigation measures to reduce the vulnerability and risk associated with flying glass during an explosive event. Options to consider include, but are not limited to, anti-shatter film, blast curtains, bullet-resistant glass, and laminated glass.*
2. Are door hinges exposed and vulnerable to tampering?			*FEMA, 2003, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426), section 3.3.3, p. 3-20 to 3-30, December, http://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf, accessed May 20, 2014.*
3. Are these doors and windows fitted with quality locks to restrict tampering and access?			*FEMA, 2003, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426), section 3.3.3, p. 3-20 to 3-30, December, http://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf, accessed May 20, 2014.*

4. Is the glass in a door, or within 3 feet from the door lock, resistant to breaking?			*Apply anti-shatter film to existing glass to provide fragment retention and reduce the overall velocity of glass fragments at failure, especially near regularly occupied and mass-gathering areas. Anti-shatter film may mitigate the impact of wind-blown debris and seismic stress in addition to explosive force by preventing pieces of broken glass from becoming lethal projectiles.*
5. Are all locks in good working order?			*Ensure all locks are in good working order; replace any locks that could be susceptible to tampering or vandalism.*
6. Are security/screen doors installed?			*FEMA, 2003, Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426), section 3.3.3, p. 3-20 to 3-30, December, http://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf, accessed May 20, 2014.*
7. Are windows fitted with quality locks to restrict access and able to be locked in a partially open position?			*Secure components of the electrical system outside of the facility against unauthorized access, for example, with door locks.*
8. Do windows have security film, laminate, wire mesh, steel shutters, security drapes or other application that offer enhanced protection from debris, and enhanced security?			*Install protective coverings, metal grills, and/or steel mesh to harden windows against penetration.*
9. Have steps been taken to restrict easy access to the roof, to include anti-climb products?			*Explore the feasibility of upgrading to stronger fence construction. Options include anti-climb aluminum or steel chain link fencing consisting of 6- to 8-gauge welded wire fabric with a center spacing of 1/2 inch or less.*

10. Do designated employees check all doors and windows to ensure they are closed and locked at the end of the business day?			*Adopt a policy and procedure to ensure all employees check windows and doors at the beginning and end of each shift.*
11. Does the facility have a policy in place to inspect rooms such as bathrooms and supply rooms to ensure there is no one is hidden in the building before locking up?			*Adopt a policy and procedure to ensure all employees inspect restrooms, supply rooms, etc. to ensure unknown persons are hiding.*
12. Are ladders and other items that could be used to access the upper floors and/or rooftop of the facility secured?			*Ensure all ladders are locked up or secured inside the facility.*
13. Are doors periodically checked for proper operation ensuring that locks actually latch when the door is closed?			*Establish a policy and procedure to ensure all employees check locks are properly secured.*
Column Total	(__ out of 13)	(__ out of 13)	
Security Lighting			
	Yes	*No*	*Options for Consideration for all responses, as applicable*

1. Is there security lighting installed around the facility's premises including parking lots and pathways?			*Install lighting for fences, gates, and/or parking areas. Before installation, determine the appropriate type of lighting based on the overall requirements of the site and the building (for example, continuous or standby). In addition, consider operational costs, such as life-cycle costs for energy and maintenance, when designing an appropriate lighting situation, because of their effect on project sustainability.*
2. Do any of the lighting have burnt out bulbs or broken pieces?			*Visit the facility in the evenings to ensure light bulbs are fully operational, record any burnt out bulbs or broken bulbs.*
3. Does the security lighting provide adequate coverage to light darkened areas?			*Update the lighting system to ensure illumination uniformity, so that security personnel can see ahead and to the sides with an absence of dark areas caused by shadows. Lighting should be brightest in secure areas, with the light gradually less in areas adjacent to high-illumination areas.*
4. Is the lighting power panel locked and secured?			*Ensure the lighting panel is locked and secured.*
5. Are there interior lights activated during off hours?			*FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 2.4.3, p. 2-68, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.*
Column Total	(__ out of 5)	(__ out of 5)	
Landscaping			

	Yes	*No*	*Options for Consideration for all responses, as applicable*
1. Is the facility clearly visible from the street?			*Ensure clear zones are free of debris, vegetation, and any items that could provide cover and concealment. When it is impossible to have adequate clear zones because of property lines or natural or manmade features, it may be necessary to increase the height of the perimeter barrier, increase security-patrol coverage, and/or add more security lighting along that portion of the perimeter. Failure to establish and maintain a clear zone along the fence minimizes its effectiveness. Consult Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430), available at http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, for more information.*
2. Are shrubs and landscaping cut to the base of the windows or low enough to negate concealment or opportunity to plant destructive devices?			*Establish clear zones on both sides of the fence to provide an unobstructed view to enhance detection and assessment. The dimensions of clears zones may vary depending on the asset being protected and level of protection required. Provide as much open space as possible between the fence and the facility.*
3. Has the facility experienced any incidents of vandalism?			*Record all incidents of vandalism internally and externally.*
4. Are trash/recycling/storage bins secured in or away from buildings to stop them from being used as a climbing aid, to discourage arson and conceal a destructive device?			*Fennelly, L., 2013, Effective Physical Security, 4th Edition, Waltham, MA: Elsevier Inc., p. 272; Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, Introduction to Security, 9th Edition, Waltham, MA: Elsevier Inc., p. 229-239; Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 39, p. 91-113, p. 259.*
Column Total	(__ out of 4)	(__ out of 4)	

Security Alarm Systems			
	Yes	*No*	*Options for Consideration for all responses, as applicable*
1. Is the premises protected by an intrusion detection system (alarm)?			*Evaluate the weakest areas of the exterior and install IDS sensors as appropriate. The basic types of sensors used for exterior intrusion are buried-line sensors, fence-associated sensors, and freestanding sensors. The IDS should be evenly distributed throughout critical areas to ensure uniform detection around the entire length of the facility's perimeter. Sensors should be placed in locations that avoid electromagnetic, acoustic, thermal, nuclear radiation, optical, seismic, and meteorological interferences.*
2. Is the security alarm system monitored by a central station?			*FEMA, 2011, Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06), section 5.5.3.3, p. 5-49, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.*
3. Does the security alarm system have a duress function?			*Consider implementing a security alarm system which has a duress function.*
4. Does the system work properly and is it tested and serviced on a regular basis?			*(Ref: OFC #13) Develop policies and procedures to periodically test the IDS and address inadequate test results. Maintain records of test results, issues, and the resolution of identified issues.*
5. Is the security alarm system used?			*Walsh, T.J., and R.J. Healy, 2012, Protection of Assets: Physical Security, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 97-113.*
6. Are a limited number of employees familiar with the procedures for turning the intrusion detection (alarm) system on and off?			*Ensure appropriate employees are trained on how to operate the intrusion detection system.*

7. Are alarm arming and de-arming codes ever changed?			*Consider changing the alarm codes semi-annually or quarterly.*
8. Does the facility have standard operating procedures for employees responding to alarm activations during operating hours and after hours?			*Establish standard operating procedures to ensure employees are aware of how to respond to alarm activations during operating hours and after hours.*
9. Does the facility's system have a cellular or back-up power supply?			*Explore the feasibility of providing backup power to the IDS to ensure its continued operation during a loss of power to the facility.*
Column Total	(__ out of 9)	(__ out of 9)	
Closed Circuit Television (CCTV)			
	Yes	***No***	***Options for Consideration for all responses, as applicable***
1. Does the facility have CCTV equipment?			Explore the feasibility of installing a comprehensive CCTV system onsite. Site-specific factors must be considered when selecting components that comprise a particular CCTV system. For example, the size of the system, in terms of the number of cameras needed, is the minimum number required to view all electronic security system sensor detection fields. In addition, some cameras may require artificial light sources. Finally, performance criteria and physical, environmental, and economic considerations must be factored into the component selection.
2. Are the cameras actively monitored?			Evaluate the need for dedicated, trained security employees to monitor the CCTV system. Explore options to maximize the effectiveness of CCTV monitoring and observation, such as frequently rotating shifts for monitoring employees and limiting the number of cameras monitored by each employees member.
3. Do the CCTV cameras cover the			Integrate CCTV or other surveillance equipment to

entrances and exits to the facility?			facilitate remote monitoring of access points.
4. Are areas adjacent to the facility monitored by CCTV?			Evaluate CCTV coverage of the facility perimeter to determine if it meets the facility's security requirements. Explore options to increase coverage as necessary.
5. Does the facility have CCTV cameras covering critical areas, such as server rooms or cash offices?			Evaluate CCTV coverage of critical areas/SAAs to determine if it meets the facility's security requirements. Explore options to increase coverage as necessary.
6. Are CCTV images recorded, retained for future use as needed, and stored in a secure area?			Evaluate the need to record CCTV video, and select video recording and storage systems for the facility as appropriate. Upgrade the CCTV system to provide for video recording and storage. Develop a policy for the review of recorded information (e.g., periodically or only after an incident). Develop policies and procedures to periodically test the CCTV system and address inadequate test results. Maintain records of test results, issues, and the resolution of identified issues.
7. Could the facility positively identify an individual from the recorded images on the CCTV system?			If CCTV is desired to be installed, ensure that the quality of the CCTV can capture features of individuals.
8. Is the facility's CCTV system regularly inspected and maintained?			Maintain the CCTV system according to the manufacturer's recommend specifications. Develop a maintenance log to document all repairs and part replacement for the IDS. Evaluate the need for more regular updates to the CCTV system to ensure it is operating at maximum effectiveness.
9. Are there appropriate signs displayed to tell the public/warn offenders that they are being monitored and recorded?			Consider posting signs warning the public of monitoring and recording devices to mitigate the risk of possible offenders. Such as: *No Trespassing, Monitoring and Recording by CCTV, Please be advised of the use of monitoring and recording devices.*
Column Total	(__ out of 9)	(__ out of 9)	

Safes/Secure Containers			
	Yes	*No*	*Options for Consideration for all responses, as applicable*
1. Does the facility have a safe installed to secure valuable items?			Procure and utilize containers that meet the security requirements of sensitive information stored at the facility.
2. Is the safe securely anchored?			Ensure the secure container is anchored to ensure that it cannot be moved from its secure location.
3. Is the safe located in a secure area?			Locate security containers where they can be observed by security personnel during their rounds.
4. Is there CCTV coverage?			Evaluate CCTV coverage of critical areas/SAAs to determine if it meets the facility's security requirements. Explore options to increase coverage as necessary. Storage of recorded coverage is recommended for 30 days.
5. Is the area armed?			Explore the feasibility of installing door sensors for critical areas within the facility. Options may include, but are not limited to, glass breakage sensors, grid mesh, vibration sensors, magnetic contacts, and conducting tape.
6. Is the safe kept locked?			If security containers with combination locks are necessary, implement the following protocols when they are obtained: Develop a process to change all security-container combinations on a schedule (e.g., semi-annually, and annually). Develop a process to change all security-container combinations when personnel are terminated, depart from the organization, and so forth. Record and secure combinations for security containers.
Column Total	(__ out of 6)	(__ out of 6)	
Cash Handling			
	Yes	*No*	*Options for Consideration for all responses, as applicable*

1. Does the facility have established cash-handling procedures?			Develop policies and procedures to adhere to cash-handling.
2. Does the facility have a lockable cash drawer?			Install a lockable cash drawer to ensure that all money is protected while it is stored in the facility.
3. Does the facility have irregular banking procedures?			N/A
4. Is a company used to transport cash?			Consider using a service to transport money instead of employees to ensure security.
5. Is money counted out of public view?			This activity should not occur in public areas or in rooms visible from the exterior.
Column Total	(__ out of 5)	(__ out of 5)	
Keys and Valuables			
	Yes	*No*	*Options for Consideration for all responses, as applicable*
1. Does the facility maintain a key inventory?			Designate a key control officer to manage the key control program and conduct regular key inventories. Limit the use of master keys for secured sensitive or critical areas to select security personnel.
2. Are regular key audits conducted?			Ensure that keys cannot be easily duplicated. Options include patented and restricted key profiles with controlled manufacturing.
3. Are all spare keys secured?			Ensure that all spare keys are secured so that only authorized personnel have access to them.
4. Are keys and identification credentials collected upon employee termination?			Establish a key control program that includes a system for the retrieval of keys from terminated personnel and a formal inventory of key assignments.
5. Does employees have a location to secure their personal items?			Consider establishing a secure location for employee's personal items.

6. Does this location have restricted access?			Ensure that this location has restricted access to employees only in order to ensure the safety of employee's personal items.
Column Total	(__ out of 6)	(__ out of 6)	
Information Security			
	Yes	*No*	*Options for Consideration for all responses, as applicable*
1. Does the facility lock away all business documents at the close of the business day?			Identify, mark, and protect sensitive information. Consult Building Security in the Digital Economy, available at http://www.ready.gov/sites/default/files/documents/files/building_security_in_digital_economy.pdf, and Protecting Aggregated Data, available at http://www.ready.gov/document/protecting%C2%A0aggregated%C2%A0data, for more information. Secure all sensitive information as appropriate (e.g., locked file cabinets, locked room).Create policies and procedures to adequately destroy sensitive information (e.g., shredding, burning).
2. Does the facility have a clear-desk policy for non-working hours?			Consider developing a procedure that requires employees to have a clean working space during non-working hours. This will ensure that confidential documents are not in plain view.
3. Does the facility have a policy requiring employees to log-off, shutdown and secure all computers			Consider implementing a policy that requires employees to log off and shutdown computers at the end of each work day to protect the integrity of computer systems

at the end of the business day?			and any sensitive information stored on them.
4. Are all computers password protected?			Ensure that all computers are password protected to ensure that information contained is protected.
5. Are computer passwords changed regularly?			Consider changing computer passwords regularly to avoid potential hacking situations. This will harden cyber security.
Column Total	(__ out of 5)	(__ out of 5)	
Communications			
	Yes	***No***	***Options for Consideration for all responses, as applicable***
1. Does the facility have a written security policy?			Develop a comprehensive security plan specific to the facility. The plan should address issues such as the following: protection of employees, contractors/vendors, visitors, and executives; protection of sensitive information; protection of funds; facility access control procedures; suspicious activity reporting procedures; employee termination procedures; parking; mail security; background checks; prohibited items; security force; end-of-day security checks; control and accountability of equipment (including keys); electronic security systems (including CCTV); physical security inspection programs; and employee security awareness training programs. Train personnel on the plan, and exercise the plan at least once a year.
2. Is the policy regularly reviewed and updated?			Review the security plan annually with local law enforcement and other first responders as necessary, to ensure these agencies are familiar with the facility and its security plans, policies, and procedures. Develop and implement procedures to review the security plan, especially any revisions that have been implemented

			within the past year, with local law enforcement on an annual basis.
3. Does the facility regularly meet with employees to discuss security issues?			Ensure key personnel are aware of, and have a copy of, the security plan. Develop a formal security awareness training program to educate all personnel on their security-related responsibilities. Include in the program topics such as the following: procedures for reporting suspicious activity, security incident (e.g. bomb threat, active shooter) response procedures, access control, and end-of-day security checks. Document the completion of training for all employees. Train all personnel on the security plan annually. Consult the Ready.gov Website for more information on training, at http://www.ready.gov/business/implementation/training . Train employees to do the following: identify their responsibilities under the facility's security program; recognize connections between the security program's objectives and selected security measures; remain familiar with resources for carrying out security-related responsibilities; and be prepared for security incidents. Consult the Ready.gov Website for more information on training, at http://www.ready.gov/business/implementation/training .
4. Does the facility encourage employees to raise their concerns about security?			Train employees to identify indicators of risk or danger and how to respond appropriately. Train employees on suspicious activity reporting procedures, security incident (e.g. bomb threat, active shooter) response procedures, procedures for suspicious packages, access control, and end-of-day security checks. For more information, visit the Ready.gov Website at

			http://www.ready.gov/business/implementation/emergency. Enhance the level of employee security awareness through the distribution of a security-related newsletter, emails, and posters that address threats, concerns, training opportunities, security initiatives, and problem areas. Consult The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management, available at https://iacd.iac.anl.gov/document/,DanaInfo=www.ready.gov+critical-success-factor-method-establishing-foundation-enterprise-security-management-0, for more information.
5. Does the facility interact with law enforcement and neighboring businesses/facilities on issues of security and crime trends?			Coordinate the security plan with local law enforcement. Consult The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management, available at http://www.ready.gov/document/critical-success-factor-method-establishing-foundation-enterprise-security-management-0, for more information. Establish a liaison and regular communication with local law enforcement and other first responders, State and Federal law enforcement and counterterrorism agencies, and industry organizations to engage in information sharing, clarify response actions, track threat conditions, and support investigations. Share critical information about the facility (e.g., floor plans, the location of critical assets or areas, notification and contact lists) with local law enforcement and emergency responders.
6. How does the facility communicate with outside first responders?			Establish an MOU/MOA with the agency to define the assistance and special services the agency will provide in the event of a threat, attack, or incident. An MOU/MOA can address items such as points of contact, notification procedures, exchange of threat information, access to the facility, hazards present on the facility, and participation in regular consults, drills, and exercises.

			Establish a liaison with the agency. Explore the option of creating a formal agreement for assistance and special services. Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout. Establish annual onsite visits for first responders to maintain their familiarity with the facility. Collaborate with the agency on potential solutions to achieve cost-effective interoperable communications onsite. Explore the option of an interconnect system, such as a gateway that can allow communication between radio systems that are otherwise incompatible because they operate on different frequency bands or using different technologies. Share critical information about the facility (e.g., floor plans, the location of critical assets or areas, notification and contact lists) with local law enforcement and emergency responders.
Column Total	(__ out of 6)	(__ out of 6)	
Emergencies			
	Yes	***No***	***Options for Consideration for all responses, as applicable***
1. Are the facility's telephones pre-programmed with emergency contact numbers?			Ensure all telephones are pre-programmed with emergency contact numbers in case of emergency.
2. Are the facility's telephone lines protected from being compromised?			Explore the feasibility of separating the communications service connections so they enter the facility in different locations. This will reduce the likelihood that an incident in one location would disrupt all facility communications systems. Explore the feasibility of implementing protective measures to the facility/building in which communications service connections terminate. Secure terminal points for communications service connections against unauthorized access, for example, with door

			locks and/or card readers. Evaluate the need to implement enhanced protective measures for terminal points to communications service connections, such as intrusion detection sensors and CCTV. Explore the feasibility of relocating the communications service connections to help mitigate the risk that the catastrophic failure of one utility could inadvertently take down another. Determine the communications service requirements to support facility core operations, and develop commensurate plans in collaboration with the provider to ensure service is restored with priority, or alternate service provisions are made. Ensure plans address legitimate hypothetical scenarios that would result in service loss and corresponding restoration timelines so the facility can address business continuity and interim workarounds.
3. Are employees thoroughly trained on how to manage emergencies?			Ensure key personnel are aware of, and have a copy of, the security plan. Develop a formal security awareness training program to educate all personnel on their security-related responsibilities. Include in the program topics such as the following: procedures for reporting suspicious activity, security incident (e.g. bomb threat, active shooter) response procedures, access control, and end-of-day security checks. Document the completion of training for all employees. Train all personnel on the security plan annually. Consult the Ready.gov Website for more information on training, at http://www.ready.gov/business/implementation/training . Train employees to do the following: identify their responsibilities under the facility's security program; recognize connections between the security program's objectives and selected security measures; remain familiar with resources for carrying out security-related responsibilities; and be prepared for security incidents.

			Consult the Ready.gov Website for more information on training, at http://www.ready.gov/business/implementation/training.
4. Are employees trained to report maintenance problems and Occupational Health and Safety concerns?			Ensure that all employees feels understands protocol for report maintenance problems and Occupational Health and Safety concerns and encourage them to do so if there is an issue.
5. Have local first responders toured the facility?			Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout. Establish annual onsite visits for first responders to maintain their familiarity with the facility.
6. Are special/significant events held at the facility?			Ensure all employees are aware of special events that occur at the facility. Establish policies and procedures to ensure all events are handled properly.
7. Are local first responders aware of the increase in population and/or potential threats?			Communicate regularly with local law enforcement and emergency personnel to ensure that they are kept up to date with out of the ordinary operations of the facility in case of an emergency situation.
Column Total	(__ out of 7)	(__ out of 7)	
Property Identification			
	Yes	*No*	*Options for Consideration for all responses, as applicable*

1. Has the facility recorded make, model and serial numbers of the facility's business items of significant value?			Consider recording all asset inventory to ensure all equipment is accounted for.
2. Are valuable property permanently marked with a unique identifier?			Consider recording all asset inventory to be marked with a unique identifier.
3. Does the facility have an inventory and visual documentation of property and equipment?			Regularly inventory all valuable items in order to understand potential risk and discourage theft.
4. Does the facility have insurance?			Ensure that the facility has insurance in case of emergency.
Column Total	(__ out of 4)	(__ out of 4)	

Total of "Yes" Answers	Total of "No" Answers
____ out of 100	____ out of 100

Grade out of 100: