



FACILITY SELF-ASSESSMENT TOOL



EXECUTIVE SUMMARY

Recent events serve as a reminder that small venues where the public gathers, which have limited security and free movement, are often targets of choice for terrorists. Each year, New Jersey State and county infrastructure partners receive numerous requests for security assessments from small businesses and nonprofit organizations. The New Jersey State Police, in collaboration with the New Jersey Office of Homeland Security and Preparedness and in cooperation with New Jersey's County Critical Infrastructure partners, prepared this Facility Self-Assessment Tool to assist organizations with identifying their security vulnerabilities.

This Facility Self-Assessment Tool is designed to assist organizations with identifying their security vulnerabilities. There is no right or wrong answer for these questions, but the honest answers will assist with establishing a more accurate assessment. By answering a series of security-related questions, users can quickly identify areas for improvement. Questions that receive a check in the "No" box may identify a potential vulnerability for the facility. Once a facility identifies a potential vulnerability, facility management may establish or adjust an internal policy or procedure or seek appropriate professional guidance to explore options available to address the vulnerability. Ultimately, the follow-up actions and next steps are based solely on each organization.

For additional resources and information, please contact the New Jersey State Police Critical Infrastructure Bureau at njroicipu@njsp.org or the New Jersey Office of Homeland Security and Preparedness Infrastructure Security Bureau at infrastructuresecurity@njohsp.gov.

Developed January 2020-Updated May 2021

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

SECTION 1: ORGANIZATION & CONTACT PERSON INFORMATION

Organization Name		Main Telephone Number	
Address (Number & Street, City, State, Zip Code)			County
Facility Type (Short description of the organization's ideology, beliefs, and mission)			
Primary Contact Person's Name		Primary Contact Person's Title	
Primary Contact Person's Telephone (Office/Mobile)		Primary Contact Person's Email	
Secondary Contact Person's Name		Secondary Contact Person's Title	
Secondary Contact Person's Telephone		Secondary Contact Person's Email	

SECTION 2: ASSESSMENT INFORMATION

Has this facility ever been assessed for security? <input type="radio"/> Yes <input type="radio"/> No If Yes, provide date of assessment:	
What agencies participated in the assessment?	
Has your facility had any past security issues? If so, explain	
Has a Threat Assessment ever been completed for this facility? <input type="radio"/> Yes <input type="radio"/> No If Yes, provide date of assessment:	Is your organization subject to regulatory requirements? If Yes, explain below: <input type="radio"/> Yes <input type="radio"/> No
What are your main security concerns?	

SECTION 3: FACILITY INFORMATION

What year was the facility built?	What type of structure is the facility?	Facility square footage	Number of stories
Number full-time employees	Number part-time employees	Highest population/attendance at any given time	Average population/attendance throughout the day
Does your facility have an Emergency Operations Plan (EOP)? <input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Limited			

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

NOTEWORTHY FACILITY INFORMATION:

SECTION 4: BUILDING IDENTIFICATION AND ACCESS CONTROL

1.	Is your facility visible from the street during both the day and night so that law enforcement security patrols can conduct external security checks? <i>(A well-maintained facility projects a deterrence message to criminals.)</i>	<input type="radio"/> Yes	<input type="radio"/> No
2.	Are all entrances marked in a uniform numbering system <i>(e.g., the main entrance is #1 and numbered clockwise from there)? (Marked entrances assist emergency responders in locating particular areas.)</i>	<input type="radio"/> Yes	<input type="radio"/> No
3.	Are entry points to your facility/business physically supervised? <i>(Individuals should be met or announced when they enter your building.)</i>	<input type="radio"/> Yes	<input type="radio"/> No
4.	Are staff/employee IDs returned to the appropriate department upon separation or termination?	<input type="radio"/> Yes	<input type="radio"/> No
5.	Is the building designed with a single public entrance equipped with a secured vestibule? <i>(Interior doors should only be released by security or other staff after vetting the visitor.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
6.	Are bollards placed along the roadway or curb line in front of the building? <i>(Bollards aid in preventing vehicles from gaining access to exterior walls, windows, and doors or in areas where vehicles are prohibited.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
7.	Do all your staff, volunteer leaders, visitors, and vendors wear identification credentials while on premises? <i>(Use of visible identification allows for rapid evaluation of individuals in sensitive areas.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
8.	Are visitors allowed entry to your building by appointment only, and do they have to report to a reception area prior to entry?	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
9.	Are visitors escorted to and from their destination? <i>(A visitor management policy helps prevent individuals from accessing unauthorized areas or information.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
10.	Are visitors asked to provide proof of identification? <i>(This technique helps prevent misrepresentation of individuals claiming to be utility workers, law enforcement, etc. When in doubt, verify with the respective agency.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
11.	Are visitors provided with visitor passes?	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
12.	Are visitor passes numbered and a record kept of who was issued the corresponding visitor pass?	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
13.	Are visitor passes designed to look different from staff identification? <i>(Different forms of identification should be easily distinguishable from a distance.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A
14.	Does your staff challenge or offer assistance to people not wearing a visitor pass? <i>(This technique is an effective security measure. It demonstrates that the staff is aware and security conscious.)</i>	<input type="radio"/> Yes	<input type="radio"/> No <input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

15. Are visitor passes collected when they leave the building? <i>(Retrieval of visitor passes helps prevent compromise or reuse of passes.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
16. Are visitor passes printed with an expiration date?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
17. Are visitors prevented from accessing unauthorized areas such as utility, mechanical, and electrical rooms and other sensitive areas? <i>(Signage, observation, and locked doors help discourage visitors from accessing restricted areas.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
18. Are all incoming deliveries inspected before being delivered to the designated recipient?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
19. Are mail and package handling procedures, to include suspicious package protocols, posted in a conspicuous location?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
20. Have you taken steps to restrict access to the roof? <i>(The roof may be used as a point of entry.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
21. Does your facility have a policy in place to inspect rooms such as bathrooms and supply rooms to ensure that there is no one hidden in the building before locking up? <i>(A criminal technique is "to stay behind" and wait for staff to depart.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
22. Are ladders and other items potentially used to access the upper floors and/or rooftop of your facility secured? <i>(Contractors or staff often leave items outside that may be used by criminal elements to gain entry.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 5: SECURITY PERSONNEL

1. Does the facility have a security force or security team to conduct daily security operations?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2. Are security personnel armed?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3. Does the facility provide security personnel with security-related training?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4. Are security personnel trained in identifying suspicious objects, substances, and people?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5. Are security personnel equipped with communications equipment?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6. Do security personnel have Standard Operating Procedures formalizing roles and responsibilities?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7. Does the facility increase security for large events or mass gatherings?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 6: FENCES AND GATES

1. Does your site have perimeter fencing that is free of visual obstructions <i>(such as brush, bushes, containers, etc.)</i> and clearly delineates the premises boundary? <i>(A well-maintained fence is a psychological deterrent to curb criminal activity.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2. Are your fences constructed at a height to limit access? <i>(six- to eight-foot-high fences provide theft security.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3. Are your gates in good working order and able to be secured by a locking mechanism?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4. Are your security measures on gates sufficient to prevent forced entry? <i>(Reinforced or heavy-duty gates can prevent forced entry.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5. Do you have a policy that requires inspection of perimeter fencing and gates on a periodic basis?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6. Do you have a policy that requires damaged fencing and gates be fixed in a timely manner?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

7. Are "No Trespassing" signs posted at the site perimeter? (<i>"No Trespassing" signage deters unauthorized access to the facility. Signs should be placed in multiple exterior locations that clearly dictate that no trespassing is permitted.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
--	--

SECTION 7: SECURITY LIGHTING

1. Is security lighting installed around the premises, including parking lots and pathways? (<i>Effective security lighting discourages criminals and aids in the detection of unauthorized individuals.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
2. Does your security lighting work properly? (<i>Visit your facility at night and check for burned-out bulbs or damaged, misaligned fixtures.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
3. Does your security lighting provide adequate coverage? (<i>Dark areas provide concealment for intruders. Effective security lighting is overlapping to reduce gaps. Security cameras may be synchronized to motion detection lighting systems.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
4. Is the lighting power panel locked and secured? (<i>Easily accessible control panels negate your security lighting plan and provide criminals a marked advantage.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
5. Are interior lights activated during off hours? (<i>Interior lighting allows for security/police patrols to detect intruders inside a facility during hours of darkness.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
6. Do you have a policy that requires replacing existing burnouts and a maintenance program wherein light bulbs are replaced at 80 percent of their recommended life?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A

SECTION 8: LANDSCAPING

1. Are shrubs and landscaping cut to the base of the window or lower? (<i>Well-maintained landscaping prevents individuals from concealing themselves or destructive devices near your facility. Also, well-maintained landscaping aids security patrols or law enforcement to effectively observe the building's exterior.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
2. Has your facility experienced any incidents of vandalism or painting of graffiti? (<i>Removal of graffiti sends a message the facility is maintained and security conscious. Contact law enforcement immediately to report any incidents.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
3. Are trash, recycling, or storage bins secured or away from the building? (<i>These containers provide ready-made climbing aids for criminals, are frequently targets of arson attacks, and are an ideal location to conceal destructive devices.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A

SECTION 9: DOORS AND WINDOWS

1. Are your door and window frames constructed of solid materials? (<i>Lesser quality doors and windows are quickly breached and do little to prevent an intruder from gaining "access".</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
2. Are door hinges exposed and vulnerable to tampering? (<i>Exposed hinge pins can be quickly "popped," allowing the door to be breached.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
3. Are doors and windows fitted with quality locks to restrict tampering and access?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
4. Is door glass shatter resistant or located farther than 3 feet from the door lock?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
5. Are all locks in good working order? (<i>Locks on doors and windows should be checked frequently for correct function. Periodically check for signs of tampering.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
6. Does your facility have security doors? (<i>Security doors offer an additional level of protection.</i>)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

7.	Do your windows have security film, laminate, wire mesh, steel shutters, drapes, or other enhanced security protection? <i>(Glass can become deadly shrapnel in the event of an explosive blast or severe weather event. These enhanced security protections make it more difficult for intruders to gain entry by simply breaking the glass.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
8.	Do you have designated staff to ensure all doors and windows are closed and locked at the end of the business day? <i>(Staff should physically check the status of the doors and windows.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9.	Are doors periodically checked for proper operation, ensuring locks properly latch when closed? <i>(Service and maintain all doors. A comprehensive maintenance program should be in place to maintain all doors and door hardware.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 10: INTRUSION DETECTION SYSTEMS

1.	Is your facility protected by an intrusion detection system?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2.	Is your security alarm system monitored by a central station? <i>(An unmonitored alarm is an ineffective prevention tool.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3.	Does your security alarm have a duress function? <i>(Consider panic alarms for reception areas, sensitive areas such as classrooms, and offices of facility leadership.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4.	Does your system work properly and is it tested and serviced on a regular basis? <i>(Alarm systems require maintenance and upgrading during their life cycle.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5.	Is your security alarm system activated? <i>(Alarm systems must be turned on and activated.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6.	Are a limited number of staff familiar with the procedures for activating and deactivating the system? <i>(Limiting the number of staff who know how to manipulate the system helps minimize compromise of the system.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7.	Are alarm codes changed on a periodic basis? <i>(Change alarm codes on a periodic basis or as staff separate to maintain integrity of the system.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
8.	Do you have Standard Operating Procedures for staff responding to alarm activations during and after operating hours? <i>(Staff could be walking into a potentially dangerous situation, and they should be aware of the proper procedures.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9.	Does your system have a cellular or backup power supply? <i>(Criminal elements have been known to disrupt the power supply to facilities prior to attempting to gain entry. Also, extended power outages could impact your facilities' security.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 11: VIDEO SURVEILLANCE SYSTEM

1.	Do you have a video surveillance system installed? <i>(A camera system allows for enhanced detection of intruders, is a psychological deterrent, and is an aid for post-incident investigation.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2.	Are cameras actively monitored? <i>(An unmonitored system only serves to document events and does not provide increased warning or command and control during incidents.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3.	Do your cameras cover all entrances and exits of the facility?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4.	Do you have video surveillance of areas adjacent to your facility, such as parking lots? <i>(Cameras in these areas may detect preoperational surveillance or preparation.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5.	Do you have cameras covering critical areas inside of your facility, such as server rooms or cash offices?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6.	Is your video surveillance system equipped with a digital video recorder (DVR) or network video recorder (NVR) with storage capability of a minimum of 60 days?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7.	Does local law enforcement have the ability to remotely access the video feed?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

8.	Do key administrators and stakeholders have the ability to remotely access the video feed?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9.	Can you positively identify an individual from the recorded images on your video surveillance system? <i>(Grainy, washed-out images do little to aid police in identifying the suspects.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
10.	Is your video surveillance system regularly inspected and maintained? <i>(Regular maintenance and function checking of the system is essential to the system's effectiveness.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
11.	Do you have signs displayed informing the public/warning offenders they are being monitored and recorded? <i>(Signs act as a deterrent for criminal activity.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 12: KEYS AND VALUABLES

1.	Do you maintain a key inventory and are keys numbered rather than named? <i>(If a key is lost or misplaced, a "named" key informs the finder exactly what it opens, whereas numbered key is more discrete.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2.	Do you regularly conduct key audits and is the key audit log secured?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3.	Are your spare keys secured and are your keys to the safe adequately secured?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4.	Are your keys, identification credentials, and uniforms collected upon employee separation?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5.	Does your staff have a location to secure their personal items and is this location secure?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 13: INFORMATION SECURITY

1.	Do you store and lock all business documents at the close of business day?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2.	Do you have a clear-desk policy? <i>(Sensitive/personal materials should be secured and not left in the open.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3.	Has your organization had a cybersecurity assessment performed in the last 12 months? <i>(It is recommended to have a cybersecurity assessment performed every 12 months by a credible third party or contact the New Jersey Cybersecurity and Communications Integration Cell.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4.	Does your organization have dedicated staff in charge of cybersecurity?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5.	Does your organization have a cybersecurity policy? <i>(This can include requiring employees to log off, shut down, and secure all computers at the end of the business day.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6.	Does your organization have a cybersecurity incident response plan?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7.	Are all your computers password protected?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
8.	Do you require computer passwords be changed regularly?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9.	Does your organization have a two-factor authentication for logging into networks? <i>(This adds a second level of protection to prevent unwanted access to networks.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
10.	Do employees complete regular cyber awareness trainings?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
11.	Does your organization take a multilayered approach to data backups and periodically test the backup media and recovery processes? <i>(Backup data sets should be kept on site, stored in the cloud, and on removable media.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
12.	Does your organization have protection software on systems and devices on the network? <i>(This can include antivirus software, web-filtering, automatic patches, and a firewall.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
13.	Does your organization maintain security and event logs for networks? <i>(The collection and review of event logs can profile normal activity, detect potential cyber attacks, and assist in performing post-breach forensics and remediation.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

SECTION 14: PROPERTY IDENTIFICATION

1. Have you recorded make, model, and serial numbers of your business items of significant value, such as mobile phones, computers, etc.?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2. Is all valuable property permanently marked with a unique identifier?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3. Do you have an inventory and visual documentation of property and equipment? Are your property lists and photographs adequately secured? <i>(Pictures and inventories aid in the recovery of stolen property.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 15: CASH HANDLING

1. Do you have established cash-handling procedures? <i>(Cash is a desired target of criminals, and it is not recommended to keep large amounts of cash in your facility.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2. Do you have a lockable cash drawer?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3. Do you have irregular banking procedures? <i>(Setting a pattern of depositing or moving cash from your facility provides criminals with opportunity.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4. Do you use an outside company to transport cash? <i>(This may be preferable and a more secure means of moving money.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5. Is money counted out of public view? <i>(Counting money should not occur in public areas or rooms visible from the exterior of the facility.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

SECTION 16: COMMUNICATION

1. Do you have written security policies and procedures?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2. Are your policies and procedures reviewed regularly and updated when necessary? <i>(Plan development should occur prior to a crisis.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3. Are policies reviewed with new hires?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4. Does the facility have a public-address (PA) system that is audible in ALL areas?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5. Does staff know how to operate the PA system?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
6. Do you regularly meet with staff and discuss security issues?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7. Do you encourage staff to raise their concerns about security? <i>(Staff members are the frontline "sensor" to detect and react to security breaches.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
8. Do you interact with law enforcement and neighboring businesses/facilities on issues of security and crime trends that might affect everyone? <i>(Establishing these relationships allows for mutual security and crime-fighting efforts.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9. Do you and your staff know the various methods of contacting authorities such as police, fire, and emergency services?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
10. Does the organization's website provide detailed information on the location of the management team, schedules, and children's activities? <i>(Too much information on the Internet could be used for nefarious purposes.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

SECTION 17: EMERGENCIES

1.	Are your telephones preprogrammed with emergency contact numbers?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
2.	Does staff know how to call emergency services via facility telephones? <i>(Ensure staff/employees are aware of procedures for dialing outside lines.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
3.	Are the preprogrammed emergency contact numbers tested periodically?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
4.	Are your telephone lines secured? <i>(Criminals have been known to target phone lines to disable alarm systems and hamper communication efforts.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
5.	Are staff trained and have they practiced their response to handle the following emergencies:			
	• Nuisance phone calls	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Active shooter	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Lockdown	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Shelter in Place	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Evacuation	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Severe weather	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Hazardous environmental conditions	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Bomb threats	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Suspicious bags/packages	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Fire	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Workplace Violence	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Insider Threat	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	• Medical Emergencies	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
	<i>(A trained and rehearsed staff is likely to perform at a higher level during crisis situations if they are trained and rehearsed prior to an event taking place.)</i>			
6.	Are staff trained to report maintenance problems and occupational health and safety concerns? <i>(Staff should be encouraged to report security deficiencies.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
7.	Have local first responders toured your facility to gain a greater understanding of the physical layout?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
8.	Are special events held at your facility that would draw large crowds or pose iconic significance?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
9.	Are local first responders aware of the increase in population due to special events and/or potential threats?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
10.	Do other groups or organizations rent or utilize your facility?	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A
11.	Are these groups or organizations required to follow your emergency plans? <i>(Having these groups or organizations sign a memorandum of understanding (MOU) ensures the continuity of security for your facility.)</i>	<input type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> N/A

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

SOURCES

1. **US Department of Homeland Security Website:** <http://www.dhs.gov/index.shtm>
2. **FEMA 452 Risk Assessment: A How to Guide to Mitigate Potential Terrorist Attacks Against Buildings:**
[FEMA452_cvr.indd](#)
3. **FEMA 426 Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings:**
[FEMA-426 / BIPS-06: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings \(dhs.gov\)](#)
4. **FEMA 430 Site and Urban Design for Security:**
[FEMA 430 Site and Urban Design for Security \(wbdg.org\)](#)
5. **FEMA 459 Incremental Protection for Existing Commercial Buildings from Terrorist Attack:**
[FEMA 459 Incremental Protection for Existing Commercial Buildings from Terrorist Attack \(wbdg.org\)](#)
6. **New Jersey Cybersecurity and Communications Integration Cell (NJCCIC):**
<https://www.cyber.nj.gov/>

RESOURCES

New Jersey Office of Homeland Security and Preparedness:

www.njhomelandsecurity.gov/resources

Active Shooter Information:

www.njhomelandsecurity.gov/active-shooter-response

Emergency Preparation:

www.ready.gov

Federal Emergency Management Agency:

www.fema.gov

New Jersey Office of Emergency Management:

www.ready.nj.gov

Mail Handling:

[Publication 166 - Guide to Mail Center Security \(usps.com\)](#)

FEMA IS-906 Workplace Security Awareness Training:

www.training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-906

FEMA IS-913.A Critical Infrastructure Security and Resilience:

Achieving Results through Partnership and Collaboration:

[FEMA - Emergency Management Institute \(EMI\) Course | IS-913.A: Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration](#)

NJCCIC Cybersecurity Guides:

www.cyber.nj.gov/learn/technical-guides/#mitigation-guides

US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA):

[Securing Public Gatherings | CISA](#)

[Insider Threat Mitigation | CISA](#)

[Power of Hello Resources | CISA](#)

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

— ADDITIONAL INFORMATION —

*Use this section to provide additional facility information or to further elaborate on a question.
Identify the section and question number.*

— OPTIONS FOR CONSIDERATION —

Use this section to record identified issues and concerns and potential security enhancement options for consideration.

Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:
Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:
Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:

Facility Self-Assessment Tool

Date of Assessment:

Completed By:

Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:
Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:
Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:
Number and Label Photograph:	Number and Label Photograph:	Number and Label Photograph:

The undersigned has reviewed the assessment and concurs with the identified vulnerabilities and recommended security enhancements:

Name:

Title:

Agency:

Signature

Date