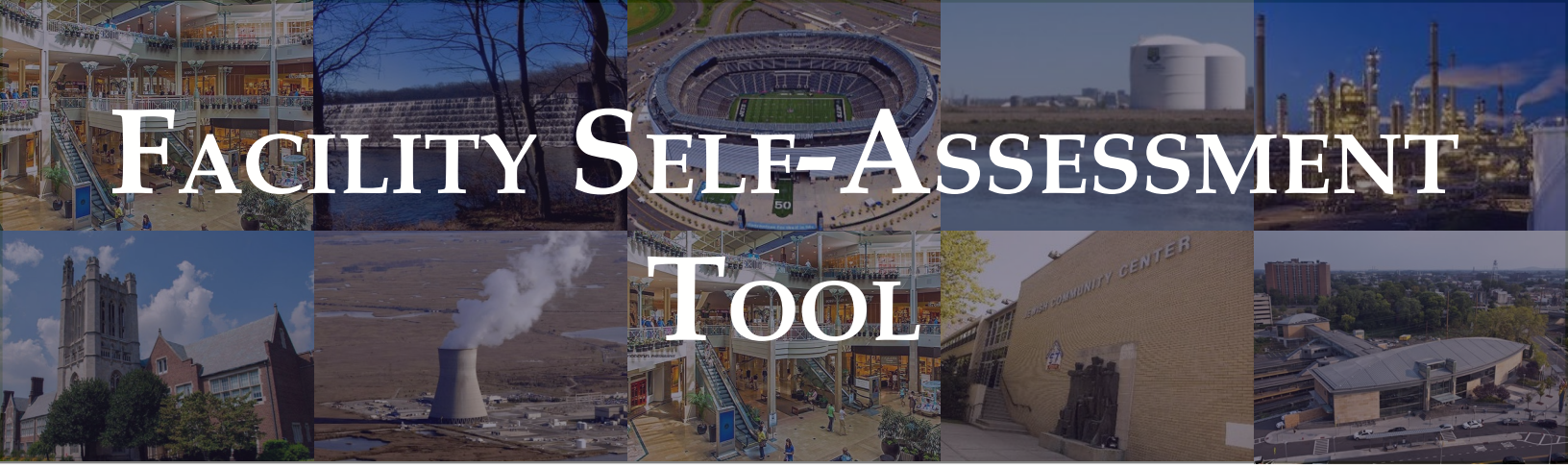

FACILITY SELF-ASSESSMENT TOOL

EXECUTIVE SUMMARY

In September 2016, the series of bombings that occurred in Seaside Park and Elizabeth, New Jersey and New York City were a stark reminder of the threat we face from individuals who want to disrupt our way of life. This event, combined with the horrific shooting in Orlando and other brutal attacks abroad in 2016, 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, the New Jersey Office of Homeland Security and Preparedness (NJOHSP) receives numerous requests for security assessments from small businesses and non-profit organizations. N JOHSP, i n cooperation with New Jersey's County Critical Infrastructure Coordinators and Risk Mitigation Planners, has prepared this Facility Self-Assessment Tool to assist organizations with identifying their security vulnerabilities.

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.

For additional information concerning this tool please contact NJOHSP's Infrastructure Security Bureau at InfrastructureSecurity@njohsp.gov.

Updated January 2019

Building Identification and Access Control	
1. Is your facility visible from the street during both the day and night so that police/security patrols can conduct external security checks? *(A well-maintained facility projects a deterrence message to criminals.)*	**Yes** ☐ **No** ☐
2. Are entry points to your facility/business supervised? *(Individuals should be met, or announced, when they enter your building.)*	**Yes** ☐ **No** ☐
3. Do all of your staff, visitors, and vendors wear identification credentials while on premises? *(Use of visible identification allows for rapid evaluation of individuals in sensitive areas.)*	**Yes** ☐ **No** ☐
4. Are visitors allowed entry to your building by appointment only, and do they have to report to a reception area before entry?	**Yes** ☐ **No** ☐
5. Are visitors escorted to and from their destination? *(A visitor management policy helps prevent individuals from wandering around your facility gathering information that could be used later for illicit purposes.)*	**Yes** ☐ **No** ☐
6. Are visitors asked to provide proof of identification? *(This technique helps prevent misrepresentation of individuals claiming to be utility workers, police officers, etc. When in doubt, verify with the responsible agency.)*	**Yes** ☐ **No** ☐
7. Are visitors provided with visitor passes?	**Yes** ☐ **No** ☐
8. Are visitor passes designed to look different from staff identification?	**Yes** ☐ **No** ☐
9. Do you have external and internal signage to guide visitors? *(Signs direct visitors where to go and deter visitors from wandering around or getting lost.)*	**Yes** ☐ **No** ☐
10. Are visitor passes collected from visitors when they leave the building? *(Retrieval of visitor passes helps prevent compromise or re-use of passes for ulterior motives.)*	**Yes** ☐ **No** ☐
11. Are visitor passes printed with an expiration date?	**Yes** ☐ **No** ☐
12. Are visitors prevented from accessing unauthorized areas such as utility rooms and sensitive areas? *(Signage, observation, and locked doors should discourage visitors from accessing restricted areas.)*	**Yes** ☐ **No** ☐
13. Do your staff challenge or offer to assist people not wearing a visitor's pass or identification credential? (*This technique is an effective security measure. It demonstrates that the staff is aware and security conscious.)*	**Yes** ☐ **No** ☐
14. Are all incoming deliveries inspected before being delivered to the designated recipient?	**Yes** ☐ **No** ☐
15. Are mail and package handling procedures posted in a conspicuous location?	**Yes** ☐ **No** ☐

Fences and Gates	
1. Does your site have perimeter fencing that is free of visual obstructions (such as brush, bushes, containers, etc.) and clearly delineates the premises boundary? *(A well-maintained fence is a psychological deterrent to curb criminal activity.)*	**Yes** ☐ **No** ☐
2. Are your fences constructed at a height to limit access? *(Six to eight foot high fences provide theft security.)*	**Yes** ☐ **No** ☐
3. Are your gates in good working order and able to be secured by a locking device?	**Yes** ☐ **No** ☐
4. Are your security measures on gates sufficient to prevent forced entry? *(Reinforced or heavy-duty gates can prevent forced entry.)*	**Yes** ☐ **No** ☐
5. Do you have the appropriate warning signs, (e.g. No Trespassing, CCTV in Use, etc.), displayed around the perimeter of the premises? *(Security signage provides a psychological deterrent to criminal activity.)*	**Yes** ☐ **No** ☐

Security Lighting	
1. Is security lighting installed around your premises, including parking lots and pathways? *(Effective security lighting discourages criminals and aids in the detection of unauthorized individuals.)*	**Yes** ☐ **No** ☐
2. Does your security lighting work? *(Visit your facility at night and check for burned-out bulbs or damaged, misaligned fixtures, etc.)*	**Yes** ☐ **No** ☐
3. Does your security lighting provide adequate coverage? *(Dark areas provide concealment to intruders. Effective security lighting has minimal gaps. Security cameras may be synchronized to motion detection lighting systems.)*	**Yes** ☐ **No** ☐
4. Is the lighting power panel locked and secured? *(Easy access to these controls negates your security lighting plan, and provides criminals a marked advantage.)*	**Yes** ☐ **No** ☐
5. Are there interior lights activated during off hours? *(Interior lighting allows for security/police patrols to detect intruders inside a facility during hours of darkness.)*	**Yes** ☐ **No** ☐

Doors and Windows	
1. Are your door and window frames made of solid materials? *(Lesser quality doors and windows are quickly breeched and do little to prevent an intruder from gaining access.)*	**Yes** ☐ **No** ☐
2. Are door hinges exposed and vulnerable to tampering? *(Exposed hinge pins can be quickly "popped" and the door breached.)*	**Yes** ☐ **No** ☐
3. Are doors and windows fitted with quality locks to restrict tampering and access?	**Yes** ☐ **No** ☐
4. Is door glass shatter resistant or located farther than three feet from the door lock?	**Yes** ☐ **No** ☐
5. Are all of the locks in good working order? *(Locks on doors and windows should be checked frequently for correct function. Additionally, check for signs of tampering with the function of the locks.)*	**Yes** ☐ **No** ☐
6. Does your facility have security doors? *(These may offer an additional level of protection an intruder must breech.)*	**Yes** ☐ **No** ☐
7. Are your windows fitted with locks capable of restricting access and locking in a partially open position? *(Frequently check the operation of these locks for correct function.)*	**Yes** ☐ **No** ☐
8. Do your windows have security film, laminate, wire mesh, steel shutters, security drapes or other applications that offer enhanced security and protection from debris? *(Glass can become a deadly shrapnel in the event of an explosive blast or severe weather. These applications may also make it harder for intruders to gain entry by breaking the glass.)*	**Yes** ☐ **No** ☐
9. Have you taken steps to restrict easy access to the roof, to include anti-climb products? *(The roof may be used as a point of entry.)*	**Yes** ☐ **No** ☐
10. Do you designate staff to check that all doors and windows are closed and locked at the end of the business day? *(Staff should physically check the status of the doors and windows, not just conduct a visual inspection.)*	**Yes** ☐ **No** ☐
11. 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? *(A criminal technique is "to stay behind" and wait for staff to depart.)*	**Yes** ☐ **No** ☐
12. Are ladders and other items potentially used to access the upper floors and/or rooftop of your facility secured? *(These items should be stored inside the facility. Walking the exterior of your building frequently could identify items left outside by staff or contractors that may be used by criminal elements to gain entry.)*	**Yes** ☐ **No** ☐
13. Are your doors periodically checked for proper operation, ensuring that locks actually latch when the door is closed? *(Service and maintain all doors. A comprehensive maintenance program should be in place to maintain all doors and door hardware.)*	**Yes** ☐ **No** ☐

Landscaping	
1. Can people see your premises clearly from the street? *(This makes it easier for police patrols and passersby to detect criminal activity. Additionally, is your street/building number easily read from the street during daylight and hours of darkness?)*	**Yes** ☐ **No** ☐
2. Are shrubs and landscaping cut to the base of the windows or low enough to negate concealment or opportunity to plant destructive devices? *(Well-maintained landscaping prevents individuals from concealing themselves or placing destructive devices near your facility. Additionally, security patrols or local police can more effectively observe the building's exterior to detect unauthorized individuals or devices.)*	**Yes** ☐ **No** ☐
3. Has your facility experienced any incidents of vandalism or painting of graffiti? *(Removal of graffiti sends a message that the facility is maintained and security conscious. Additionally, the police should be contacted immediately to report graffiti or vandalism.)*	**Yes** ☐ **No** ☐
4. Are your trash/recycling/storage bins secured in or away from buildings to stop them from being used as a climbing aid, to discourage arson, or to conceal a destructive device? *(These containers provide ready-made climbing aids for criminals, are frequently targets of arson attacks, and ideal places to conceal a destructive device.)*	**Yes** ☐ **No** ☐

Security Alarm Systems	
1. Is your facility protected by an intrusion detection system?	**Yes** ☐ **No** ☐
2. Is your security alarm system monitored by a central station? *(A non-monitored alarm is not an effective prevention tool.)*	**Yes** ☐ **No** ☐
3. Does your security alarm system have a duress function? *(Consider these for reception areas, sensitive areas such as classrooms, and offices of facility leadership who may be targeted.)*	**Yes** ☐ **No** ☐
4. Does your system work properly, and is it tested and serviced on a regular basis? *(Alarm systems require maintenance and upgrades during their life cycle.)*	**Yes** ☐ **No** ☐
5. Is your security alarm system used? *(In order to function, the alarm system must be turned on and employed.)*	**Yes** ☐ **No** ☐
6. Are a limited number of your staff familiar with the procedures for turning the intrusion detection (alarm) system on and off? *(Limiting the number of staff who know how to manipulate the alarm system helps minimize compromise of alarm codes.)*	**Yes** ☐ **No** ☐
7. Are your alarm arming and de-arming codes ever changed? *(On a regular basis or as staff separate, codes should be changed.)*	**Yes** ☐ **No** ☐
8. Do you have standard operating procedures for staff responding to alarm activations during operating hours and after hours? *(Staff could be walking into a potentially dangerous situation, and need to be aware of what actions to take.)*	**Yes** ☐ **No** ☐
9. Does your system have a cellular or back-up power supply? *(Criminal elements have been known to disrupt the power supply to facilities prior to attempting to gain entry. Additionally, extended power outages could impact your facilities' security.)*	**Yes** ☐ **No** ☐

Closed Circuit Television (CCTV)	
1. Do you have CCTV equipment installed? *(A camera system allows for enhanced detection of intruders, is a psychological deterrent, and is a means to document a subject's identity for police department follow-up.)*	**Yes** ☐ **No** ☐
2. Are your cameras actively monitored? *(An unmonitored CCTV only serves to document events, and does not provide increased warning or command and control during incidents.)*	**Yes** ☐ **No** ☐
3. *Do your CCTV cameras cover the entrances and exits to your building?*	**Yes** ☐ **No** ☐
4. Do you have video surveillance of areas adjacent to your facility? *(Parking lots, etc. Cameras may detect pre-operational surveillance or preparation.)*	**Yes** ☐ **No** ☐
5. Do you have CCTV cameras covering critical areas inside of your facility, such as server rooms or cash offices? *(These areas may be targeted by nefarious individuals.)*	**Yes** ☐ **No** ☐
6. Are your CCTV images recorded, retained for future use as needed, and stored in a secure area? *(Camera images may be essential to solving crimes. Criminals may seek to destroy video evidence during the commission of their activity.)*	**Yes** ☐ **No** ☐
7. Could you positively identify an individual from the recorded images on your CCTV system? *(Grainy, washed out images do little to help the police identify the suspects.)*	**Yes** ☐ **No** ☐
8. Is your CCTV system regularly inspected and maintained? *(Regular maintenance and function checking of the system is essential to the system's effectiveness.)*	**Yes** ☐ **No** ☐
9. Do you have appropriate signs displayed to tell the public/warn offenders that they are being monitored and recorded? *(These signs alone may deter criminal activity.)*	**Yes** ☐ **No** ☐

Cash Handling	
1. Do you have established cash-handling procedures? *(Cash is a desired target of criminals. It is not recommended to keep large amounts of cash in your facility.)*	**Yes** ☐ **No** ☐
2. Do you have a lockable cash drawer?	**Yes** ☐ **No** ☐
3. Do you have irregular banking procedures? *(Have you set a pattern of depositing or moving cash from your facility that criminals may exploit?)*	**Yes** ☐ **No** ☐
4. Do you use an outside company to transport cash? *(This may be preferable and safer/more secure means of moving money versus an employee.)*	**Yes** ☐ **No** ☐
5. Is money counted away from public view? *(This activity should not occur in public areas or in rooms visible from the street/exterior.)*	**Yes** ☐ **No** ☐

Keys and Valuables	
1. Do you maintain a key inventory, and are keys numbered rather than named? *(If a key is lost or misplaced a "named' key informs the finder exactly what it opens. A numbered key does not.)*	**Yes** ☐ **No** ☐
2. Do you regularly conduct key audits, and is the key audit log secured? *(This is essential to maintain control of your keys.)*	**Yes** ☐ **No** ☐
3. Are your spare keys secured, and are your keys to the safe adequately secured?	**Yes** ☐ **No** ☐
4. Are your keys, identification credentials, and uniforms collected upon employee separation?	**Yes** ☐ **No** ☐
5. Does your staff have a location to secure their personal items?	**Yes** ☐ **No** ☐
6. Does this location have restricted access?	**Yes** ☐ **No** ☐

Information Security	
1. Do you store and lock all business documents at the close of the business day?	**Yes** ☐ **No** ☐
2. Do you have a clear-desk policy? *(Are sensitive/personal materials secured and not left in the open.)*	**Yes** ☐ **No** ☐
3. Does your organization have dedicated staff/personnel in charge of cybersecurity?	**Yes** ☐ **No** ☐
4. Does your organization have a cybersecurity policy? *(This can include requiring employees to log-off, shut down, and secure all computers at the end of the business day.)*	**Yes** ☐ **No** ☐
5. Does your organization have a cybersecurity incident response plan?	**Yes** ☐ **No** ☐
6. Are all your computers password protected?	**Yes** ☐ **No** ☐
7. Do you require computer passwords to be changed regularly?	**Yes** ☐ **No** ☐
8. Does your organization have two-factor authentication for logging into networks? *(This adds a second level of protection to prevent unwanted access to networks.)*	**Yes** ☐ **No** ☐
9. Do employees complete regular cyber awareness trainings?	**Yes** ☐ **No** ☐
10. Does your organization schedule routine data backups?	**Yes** ☐ **No** ☐
11. Does your organization have protection software on systems and devices on the network? *(This can include antivirus software, web-filtering, automatic patches and a firewall.)*	**Yes** ☐ **No** ☐
12. Does your organization maintain security and event logs for networks? *(The collection and review of event logs can to profile normal activity, detect potential cyber attacks, and assist in performing post-breach forensics and remediation.)*	**Yes** ☐ **No** ☐

Property Identification	
1. Have you recorded make, model and serial numbers of your business items of significant value *(such as mobile phones, computers etc.)?*	**Yes** ☐ **No** ☐
2. Is all valuable property permanently marked with a unique identifier?	**Yes** ☐ **No** ☐
3. Do you have an inventory and visual documentation of property and equipment? Are your property lists and photographs adequately secured? *(Pictures and inventories aid in the recovery of stolen property. These lists should also be kept in a secure area/container.)*	**Yes** ☐ **No** ☐
Communication	
1. Do you have written security policies and procedures?	**Yes** ☐ **No** ☐
2. Are your policies and procedures reviewed regularly and, if necessary, updated? *(Plan development should occur prior to a crisis situation occurring.)*	**Yes** ☐ **No** ☐
3. Do you regularly meet with staff and discuss security issues?	**Yes** ☐ **No** ☐
4. Do you encourage staff to raise their concerns about security? *(Your staff is the frontline "sensor" to detect and react to security breaches.)*	**Yes** ☐ **No** ☐
5. Do you interact with law enforcement and neighboring businesses/ facilities on issues of security and crime trends that might affect everyone? *(Relationships with the police and adjoining facilities allow for a mutual security and crime fighting effort.)*	**Yes** ☐ **No** ☐
6. Do you and your staff know the various methods of contacting authorities such as police, fire, and emergency services?	**Yes** ☐ **No** ☐
7. Does the organization's website provide detailed information on the location of the management team/schedules/children's activities, names, and locations? *(Too much information on the internet about your facility could be used for nefarious purposes.)*	**Yes** ☐ **No** ☐

Emergencies	
1. 1. Are your telephones pre-programmed with emergency contact numbers?	**Yes** ☐ **No** ☐
2. *Are your telephone lines protected from being compromised? (Criminals have been known to target phone lines to disable alarm systems, and hamper communication efforts.)*	**Yes** ☐ **No** ☐
3. Are staff trained, and have they practiced their response to handle emergencies?	
Nuisance phone calls	**Yes** ☐ **No** ☐
Active shooter and lockdown shelter-in-place	**Yes** ☐ **No** ☐
Evacuation	**Yes** ☐ **No** ☐
Severe weather	**Yes** ☐ **No** ☐
Hazardous environmental conditions	**Yes** ☐ **No** ☐
Bomb threats	**Yes** ☐ **No** ☐
Suspicious bags/packages	**Yes** ☐ **No** ☐
Fire	**Yes** ☐ **No** ☐
Workplace violence	**Yes** ☐ **No** ☐
(A trained and rehearsed staff is likely to perform at a higher level during crisis situations if they are trained and rehearsed prior to the stressful event taking place.)	
4. *Are staff trained to report maintenance problems and Occupational Health and Safety concerns? (Staff should be encouraged to report security deficiencies.)*	**Yes** ☐ **No** ☐
5. Have local first responders toured your facility to gain a greater understanding of the physical layout? *(Pre-planning with local first responders increases facility security and safety.)*	**Yes** ☐ **No** ☐
6. Are special events held at your facility that would draw large crowds or pose iconic significance?	**Yes** ☐ **No** ☐
7. Are local first responders aware of the increase in population due to special events and/or potential threats? *(Special events may draw unwanted attention from individuals who do not share your views and beliefs. Additionally, large crowds could overwhelm capabilities of local first responders unless planned for.)*	**Yes** ☐ **No** ☐

Additional Resources

New Jersey Office of Homeland Security and Preparedness:
www.njhomelandsecurity.gov/resources

Active Shooter Information:
www.njhomelandsecurity.gov/active-shooter-response

Developing Emergency Plans for Houses of Worship:
www.fema.gov/media-library/assets/documents/33007

Emergency Preparation:
www.ready.gov

Federal Emergency Management Agency:
www.fema.gov

New Jersey Office of Emergency Management:
www.ready.nj.gov

Mail Handling:
about.usps.com/publications/pub166/pub166fm_003.htm

FEMA IS-906 Workplace Security Awareness Training:
www.training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-906

FEMA IS-921.A Implementing Critical Infrastructure Security and Resilience:
www.training.fema.gov/is/courseoverview.aspx?code=IS-921.a

New Jersey Cybersecurity and Communications Integration Cell (NJCCIC):
www.cyber.nj.gov

NJCCIC Private Sector Best Practices:
www.cyber.nj.gov/private-sector

Sourcing Information

American Red Cross, Ready Rating, Multi-Building Physical Security Checklist, United States of America

Cambridgeshire Constabulary, Home Security Self-Assessment, United Kingdom

Hertfordshire Constabulary, Business Premises Self-Assessment Checklist, United Kingdom

Howell Police Department, Business Security Survey, New Jersey

Jefferson City Police Department, Commercial or Business Security Survey, Missouri

Lakewood Police Department, Business Security Survey, New Jersey

National Crime Prevention Council, Business Watch Brochures, United States of America

Newark Police Department, Business Security Survey, New Jersey

Orange Police Department, Business Security Survey, New Jersey

San Diego Police Department, Small Retail Business Security Reference Material and Survey Form, California

Westerville Police Department, Security Survey Checklist: Business, Ohio

Windsor Police Department, Home or Business Property Self Audit, New Jersey