2023

Non-Profit Security Grant Program

Threat, Vulnerability & Risk Assessment Tool

FOR OFFICIAL USE ONLY

(FOUO)

- SECURITY SENSITIVE INFORMATION -

FOUO information shall not be disseminated in any manner – orally, visually, or electronically – to unauthorized personnel. The holder of the information will comply with access and dissemination restrictions. Ensure the recipient of FOUO information has valid "need-to-know" and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials or otherwise obtaining the information.

The following report is the result of a Threat, Vulnerability and Risk Assessment (TVRA) for the .

This report is specifically designed to assist organizations in their application for the United States Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) administered Non-Profit Security Grant Program (NSGP).

This assessment consists of an assessment survey conducted by , subsequent interview/consultation conducted by , and representing .

Recommendations provided through this process are intended to inform efforts to increase the prevention, protection, preparedness, mitigation, response and recovery capabilities of the facility, with the overall goal of reducing the facility's vulnerability to terrorism, crime and other all-hazard risks. The ability to deter, detect, delay and respond to an incident is critical in establishing an effective safety and security program consistent with incident management protocols designed to prevent, protect against, mitigate, respond to, and recover from a significant incident or event. The survey process provides a snapshot of the conditions at the time of the assessment based upon organizational input and is designed specifically to support the organization's efforts related to the NSGP. Safety and security efforts must be viewed as dynamic processes and accordingly, it is recommended that the organization work to implement a comprehensive strategic security framework as a component of a cohesive, professionally coordinated community-wide safety and security strategy. Regardless of results, it is recommended that organizations continually monitor their security environments and adjust security practices, policies and procedures consistent with changes in the environment.

ABOUT SCN

The Secure Community Network (SCN), a nonprofit 501(c)(3), is the official safety and security organization of the Jewish community in North America. Founded in 2004 under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations, SCN works on behalf of 146 Federations, the 50 largest Jewish non-profit organizations in North America and over 300 independent communities as well as with other partners in the public, private, nonprofit and academic sectors to ensure the safety, security and resiliency of the Jewish people.

SCN serves as the Jewish community's formal liaison with federal law enforcement and coordinates closely with federal, state and local law enforcement partners on safety and security issues related to the Jewish community; through the organization's Operations Center and Duty Desk, SCN analyzes intelligence and information, providing timely, credible threat and incident information to both law enforcement and community partners. SCN's team of law enforcement, homeland security and military professionals proactively works with communities and partners across North America to develop and implement strategic frameworks that enhance the safety and security of the Jewish people. This includes developing best practice policies; emergency plans and procedures; undertaking threat and vulnerability assessments of facilities; providing critical, real-world training and exercises to prepare for threats and hazards; offering consultation on safety and security matter; and providing response as well as crisis management support during critical incidents.

SCN is dedicated to ensuring that Jewish organizations and communities, as well as life and culture, can not only exist safely and securely, but flourish.

TABLE OF CONTENTS

We encourage you to contact the assessor with any questions related to the contents of this report.

Should you have additional questions or concerns as you look to address the findings of this process and/or implement security improvements, please contact us.

NSGPsupport@SecureCommunityNetwork.org
844.SCN.DESK (844.726.3375)

Disclaimer

The following information is the result of a TVRA. This TVRA was conducted during the COVID-19 pandemic which may have required a virtual process for interacting with the affected facility while adhering to best practices for pandemic health concerns. To the extent possible, this TVRA was conducted within the confines of both security best practices and the U.S. Department of Homeland Security's recommended protective measures.

This TVRA attempts to determine the vulnerabilities that threat actors could exploit as reported by the organization in their TVRA, and to the extent possible given current operating conditions. The vulnerabilities identified and the ultimate mitigation recommendations that are made are in response to the organization's reporting while following the TVRA tool's guidance. The mitigation recommendations which are included in the assessment are provided to coincide with increases in the organization's current security posture, fill in gaps where security is lacking and/or improve or upgrade existing security measures in order to reduce the organization's vulnerability to crime, attack and other risks. It is important to note that the recommendations given cannot guarantee that the facility will not become a victim of crimes, attacks or other risks. This TVRA process merely provides a snapshot of the identified current security conditions reported by the organization upon their completion of the TVRA and is designed specifically to support the organization's efforts related to the NSGP. The mitigation recommendations are in response to the reported TVRA and are not necessarily the result of a TVRA performed by an SCN or other security professional. Safety and security preparedness, prevention and protection efforts must be viewed as dynamic processes. Accordingly, we strongly recommend that the organization continually monitor its environment and adjust security practices, policies and procedures consistent with changes in the environment – to include a comprehensive on site TVRA conducted by SCN when health conditions permit. SCN does not assume any responsibility for the failure to detect, identify or make known any additional hazards or threats that are or may come to be known beyond what has been self-identified in this TVRA, nor responsibility for the data or information inputted into the document.

This tool was developed based on general physical security best practice and to conform with the broad requirements of the NSGP, as articulated by DHS/FEMA in past Notice Of Funding Opportunity announcements. Organizations should review the latest guidance issued by DHS/FEMA as well as their individual State Administrative Agencies (SAAs), to ensure compliance with all requirements. Organizations should pay particular attention to requirements related to assessments and the suitability and acceptance of this process by individual SAAs. SCN makes no warranties, express or implied, in connection with this tool or the performance of the same and accepts no responsibility for the use of this tool or its effectiveness, nor shall SCN be held responsible or liable for any costs, damages, or performance, or lack thereof, related to the use of this tool or any information provided therefrom.

Through an assessment process, a security professional or SCN may offer or recommend certain equipment for consideration to address the findings of this assessment. SCN is not affiliated with any manufacturers of equipment or hardware, nor does SCN receive any compensation from any manufacturer; SCN and its personnel will make equipment recommendations based solely on technical specifications and/or verified performance, if at all. SCN assumes no responsibility or liability for the use and operation of any equipment or products recommended through this tool, and whether made by members of SCN or other security professionals. This assessment and accompanying process are intended to be useful as an organization takes steps to improve the security of a facility and those who use it.

This template was created by SCN as a guide and has been made available as a general resource; SCN cannot control the use of this document by others, including but not limited to non-security professionals. As a reminder, as stated throughout this document, the purpose of this assessment is to assist in the application of the NSGP, but it – alone – may not be sufficient to meet eligibility requirements related to assessments, as articulated by an SAA. Organizations must review the latest federal and state guidance to ensure they are meeting all applicable eligibility requirements.

INTRODUCTION

SCN has supported the development of this TVRA tool for Jewish community partners. The assessment is designed using commonly recognized best practice methods and specifically to support an organization's efforts related to the NSGP, and with the purpose of the TVRA to: (1) understand the current threat environment, identify vulnerabilities, mitigate those vulnerabilities and prepare for emergencies; (2) guide the response to and recovery from emergency incidents, and; (3) enhance continuity of operations under high threat conditions.

This TVRA tool incorporates and adapts best-practice guidance and examples to aid non-profits and community organizations as well as related facilities in identifying areas of site security concerns. By answering a series of security-related practice and equipment questions, users may quickly identify potential areas of concern. When a question is answered as *"No,"* this may identify an area where enhanced attention may be warranted. Please note that not all questions will be relevant to all entities.

A common sense, pragmatic approach must be taken when using the TVRA template, as the tool adopts a "defense-in-depth" approach, and which is indicated by the core principles of *Deter, Detect, Delay, Respond.*

EXECUTIVE SUMMARY

The scope and overall objective of the TVRA is to provide a general evaluation of facility preparedness and security posture. The TVRA tool is designed to assist the organization in understanding their current threat environment and vulnerabilities within the confines of the NSGP administered by DHS and FEMA, and to seek remedies for the identified vulnerabilities via FEMA's Approved Equipment List (AEL) for the NSGP, and can be used either in a self-guided fashion or by a security professional.

The report is organized to address identified security vulnerabilities and propose mitigation measures to assist in implementing and maintaining a more robust security posture. The report provides historical threat information, identifies current vulnerabilities and recommends potential mitigation products or technologies.

This abbreviated assessment accomplishes the following:

- Complements each location's existing security initiative and improvement plans.
- Assesses security vulnerabilities considering recent events and the current threat environment targeting similar facilities and institutions.
- Assesses each location's ability to detect and respond to external and internal physical security threats.
- Determines the organization's ability to identify, respond to and mitigate basic emergencies and incidents.

USING THE TVRA TOOL

What are we protecting against? What is the threat?

In order to understand and develop a physical protection system, it is necessary to define the potential threat to the facility.

Outsider:

An "outsider" is a person or persons who are not known to the community and who do not/should not have authorized access to the facilities or location. An outsider may have the intent to harass community members, engage in vandalism, theft, destruction of facilities, critical equipment or person-on-person violence. Outsiders who pose a threat can be characterized by individuals who have specific religiously or racially based animus toward the facility or one of its members. Outsiders can also include vandals or criminal elements who may gain interest or access to the facility or its environs simply by proximity.

Insider:

An "insider" is a current or former community member, employee, volunteer, contractor etc., who has – or had – authorized access to an organization, facility, or location.

Unacceptable Consequences:

An "unacceptable consequence" is considered a threshold that an organization considers to be severe enough that they can justify spending/obtaining resources to prevent. Unacceptable consequences can vary from organization to organization and must be interpreted internally. For instance, some may consider minimal vandalism, such as graffiti and associated clean-up, an acceptable consequence versus spending resources in an attempt to deter and prevent it.

As areas of concern are identified, leadership may elect to make physical improvements, establish or adjust an internal policy, implement training or seek additional professional guidance to explore available options to address the concern(s).

SCN's TVRA tool is designed to provide a systematic method for performing a base-level security assessment of a facility. The TVRA is designed to follow security best practices for identifying threats to the facility, and ultimately identifying vulnerabilities and designing recommendations to defend against the identified threats.

The Process:

The TVRA is designed to provide the assessor with an easy-to-use tool that follows security best practices in order to understand a base-level security posture of a facility. It utilizes standard security terminology and methodology to review the facility from a defense-in-depth approach (outside/in). The assessor should follow the security questionnaire in the order the questions are presented, taking care to follow the logic of the questions, as they are designed to build off of each other – essentially walking the assessor from the facility's exterior perimeter into its inner sanctum, while taking into account each security layer during the process. It is a step-by-step, building block approach to assessing the facility.

Upon completion, the assessor will tabulate the risk score for each particular category. In this way, the TVRA provides the ability to identify not just the overall security posture for a facility, but individual areas that can be specifically identified and addressed. The next step is to complete the suggested recommendations section to address the identified vulnerabilities.

******IMPORTANT NOTE******

Specific review and guidance for the recommendations section must be provided by a member of SCN's professional security team or recognized professional Jewish Community Security Director or Regional Security Advisor to ensure that the recommendations align with the identified vulnerabilities.

Risk Scoring:

Assessors should utilize the tool to apply against their respective facility in the order in which the categories are provided; Perimeter, Lighting, Vehicle Access, Control & Parking, Exterior Doors & Windows, Access Control & Visitor Management, Video Surveillance (CCTV – Internal & External), Building Interior, Security Systems, Training & Exercises and Policies and Procedures. This outside/in approach provides a holistic methodology for assessing vulnerabilities much as an adversary would and provides the necessary insights for a defense-in-depth security posture.

In some instances, there will only be a *"yes"* or *"no"* answer.

Yes	▪ A *"yes"* score of 1 indicates that you have adequate and robust security for that question.
Some	▪ A *"some"* score of 2 indicates that you have some, but not necessarily adequate security for that question. Or, for example, *"Are property boundaries of the facility easily recognizable by visual means?"* In this instance, only *"some"* of the boundaries may be recognizable. *"Some"* allows for subjectivity by the assessor.
No	▪ An answer of *"no"* to a question means that you do not have any security measures in place related to that question.
N/A	▪ *"N/A"* means that the question does not apply to your facility or location.

Upon completion of a category, a range is given for the total score within that category. For example, in category 1 – Perimeter, it is possible to have a low-risk score of 1 - 9, a medium risk score of 10 - 18 and a high-risk score of 19 – 27. In this category, a facility operator may be willing to accept any risk score of 9 or below and choose to initiate action to reduce risk for any score of 10 or higher. Scores are aggregated and totaled for each category, as well as the entire facility, enabling both category specific and overall facility assessment.

NSGP TVRA Completion Support

Upon completion of this document, an organization should contact SCN or a professional Jewish Federation Community Security Director or Regional Security Advisor to schedule a consultation. These limited number of consultations are generally available on a first-come, first-serve basis.

During that consultation, and should one be available, a professional will work with an organization to translate your findings into recommendations, providing the foundation for an organization to complete the Investment Justification of the NSGP grant application.

This information has been prepared to help organizations in establishing a base-level assessment of the relative safety and security status of a facility. Please note that this information is intended as guidance only; some of the information presented may not meet the specific requirements of a particular facility, nor is it intended to take the place of a comprehensive, formal and professionally undertaken risk assessment and gap analysis. Organizations interested in receiving a comprehensive security assessment should contact SCN, a local Federation Community Security Director or Regional Security Advisor, if available, law enforcement or a Protective Security Advisor with the U.S. Department of Homeland Security.

THREATS TO JEWISH FACILITIES/INSTITUTIONS

FBI HATE CRIME DATA

This summary provides an overview of open source statistics regarding reported antisemitic incidents in the United States and Canada. Please note, the NSGP requires threat data specific to the applicant; this information is meant to be general and contextual in nature. It is not sufficient to effectively complete the NSGP application. All statistics included in this summary were obtained through open sources and may contain unofficial data. This summary should be considered preliminary in nature. Exact counts are subject to change pending official end-of-year data reporting.

Though the FBI numbers for 2021 seem to indicate a sharp decline in both overall hate crimes and hate crimes directed against the Jewish community, this was not the case. This decrease is believed to be due to a new reporting system in which thousands of law enforcement agencies did not implement. The 2021 FBI data do not include the overwhelming majority of hate crimes committed in California, Florida, or New York, which are home to half of the Jewish population in the U.S. It is important to note this as there have been four deadly attacks against the Jewish community since just October 2018.

For 2021, 1,013 of the 7,303 (14%) hate crimes reported to the FBI were religiously motivated. Of these, 324 (32%) were motivated in whole or in part by anti-Jewish bias. In comparison, in 2020, 683 of the 1,244 religiously motivated hate crimes (65%) were anti-Jewish, out of 8,263 hate crimes reported. Although this appears to be a dramatic decrease both in anti-Jewish crimes and overall hate crimes, see the "Significant Underreporting" section below for important context.

FBI Hate Crime Data				
Year	**Total Number of Reported Hate Crime Offenses**	**Offenses Motivated by Religious Bias**	**Percent Motivated by Anti-Jewish Bias***	**Percent Occurring at a HOW****
2021	**7,303**	1,013	39.1%	
2020	**8,263**	1,244	77.0%	
2019	**8,559**	1,650	60.2%	16.7%
2018	**8,496**	1,550	57.8%	15.4%
2017	**8,437**	1,679	58.1%	15.0%

- Of the 324 anti-Jewish hate crimes reported in 2020, 219 (68%) included property damage or vandalism, 112 (35%) intimidation, 19 (6%) simple assaults, 8 (2%) aggravated assaults, and 8 (2%) burglary or breaking and entering.

- Of the 362 locations in which the reported anti-Jewish hate crimes occurred, 77 (21%) occurred in homes, 47 (13%) on streets or sidewalks, 35 (10%) in houses of worship, 28 (8%) in schools, and 26 (7%) in parks or playgrounds.

- Of the 412 reported direct victims, 235 (57%) were individuals, 65 (16%) were businesses, 65 (16%) were government-related, 23 (6%) were religious organizations, and 18 (4%) were others.

ADL – 2021 DATA

In 2021, ADL recorded 2,717 antisemitic incidents in the United States; a 34% increase when compared to 2020. This is the highest number on record since ADL began tracking antisemitic incidents in 1979. Harassment was the most frequently reported incident type in the ADL's 2021 audit accounting for 1,776 cases; a 43% increase from 1,242 in 2020. Most concerningly, there were 88 incidents of antisemitic assault; a 167% increase from 33 in 2020. The assaults resulted in 131 victims and were all non-lethal. Additionally, there were 853 incidents were cases of vandalism, a 14% increase from 751 in 2020. In 2021, there were no assaults perpetrated against the Jewish community that resulted in mass causalities. Of the physical assaults against Jewish individuals, the vast majority (87%) were perpetrated without the use of a deadly weapon.

In 2021, the ADL reported 525 incidents at Jewish institutions such as synagogues, Jewish community centers, and Jewish schools, an increase of 61% from the 327 incidents reported in 2020.

- Of the 525 incidents, 413 were incidents of harassment, 101 were incidents of vandalism and 11 were incidents of assault.
- Of the 413 incidents of harassment, 111 were anti-Zionism/anti-Israel-focused, 42 were Zoombombings, and 24 were had an extremist nexus.

	2018	2019	2020
Assault	**39**	**61**	**31**
Harassment	**1,066**	**1,127**	**1,242**
Vandalism	**774**	**919**	751
Annual Total	**1,879**	**2,107**	**2,024**

Known extremist groups or individuals inspired by extremist ideology were responsible for 484 incidents in 2021, up from 332 incidents in 2020. This represents 18% of the total number of incidents in 2021. Of the 484 incidents attributed to hate groups or extremists, 422 took the form of antisemitic propaganda such as flyers and banners.

HOW TO READ THIS DOCUMENT

Below is a list of recommendations in order of their appearance in this report. Each recommendation has been assigned a priority level as follows:

[P1] HIGH Priority – Strongly recommended to provide the appropriate level of protection, safety and security.

[P2] MODERATE Priority – Important to maintain the appropriate level of protection, safety and security.

[P3] LOW Priority – Recommended for best-practice consideration but not critical to the maintenance of safety and security under most conditions.

SITE CHARACTERISTICS & GENERAL INFORMATION

FACILITY NAME: DATE CONDUCTED:

ADDRESS:

ASSESSMENT FINDINGS

PERIMETER

Perimeter security measures should be considered your first line of defense in a comprehensive defense-in-depth security plan. Well-defined boundaries between public and private areas can be achieved by using physical elements such as fences, architectural design and water features, pavement treatment, art, signage and landscaping to express ownership and identify intruders and individuals who do not belong. The proper application of these types of items can achieve measures of perimeter access control by incorporating deterrence and delay into the security design. In order to perform a perimeter review, the assessor must physically walk around the outer boundaries of the facility property and answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are property boundaries of the facility easily recognizable by visual means?				
2. Is there a marquee or other sign visible from the adjacent roadway that identifies the presence of the facility?				
3. Can site entry points be readily observed and monitored by staff and individuals in the facility in the course of their normal activities?				
4. Can the perimeter of the site be secured to prevent unauthorized vehicles or pedestrians from entering?				
5. Does the site have perimeter fencing that is free of visual obstructions and clearly identifies the boundary of the premises?				
6. Are the fences 6 to 8 feet high and in good condition?				
7. Are gate locks/bars sufficient to prevent forced entry?				
8. Are any exterior playgrounds fenced with a restricted entry point?				
9. Is exterior mechanical equipment reachable by vehicles protected with bollards or other devices?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-9*	*Med 10-18*	*High 19-27*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Install Perimeter Fencing to establish facility boundaries and prevent unauthorized access - 14SW-01-WALL
- Install Perimeter Fencing to establish facility boundaries and prevent unauthorized access - 14SW-01-WALL
- Install bollards or barriers to protect specific equipment, and to prevent vehicle based attacks and/or accidents - 14SW-01-WALL
- Consider employing off-duty police as security personnel during services, when the facility is open, and events - NO AEL
- Install fixed lighting to improve visibility in perimeter areas and enhance camera performance - 14SW-01-LITE
- Install Cameras systems to monitor and identify threats and suspicious activity on facility perimeter - 14SW-01-VIDA
- Install Perimeter Fencing to establish facility boundaries and prevent unauthorized access - 14SW-01-WALL

Additional Notes / Recommendations:

LIGHTING

Security lighting systems are an essential element of a physical security protection program assisting in the first line of deterrence, detection, response and defense. Security lighting systems are utilized to provide enough illumination to enable a person or a camera system to assess a security area or zone for general safety, hazards or threats. As part of the first phase of a security system, adequate lighting will not only assist with general safety awareness and threat detection, but can also serve as a psychological deterrent to nefarious activity. In order to perform a review of the facility's lighting, the assessor must physically walk around the facility in dusk and darkness conditions and answer the following questions to fully assess the facility's lighting posture.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are designated parking lots or parking areas well-lighted?				
2. Are pedestrian walkways and building entrances well-lighted?				
3. Are all sides of the building illuminated by exterior lighting?				
4. Is motion detector-activated lighting located near doors and windows?				
5. Are exterior lights checked weekly for functionality?				
6. Are exterior lighting fixtures free of obstructions by vegetation or man-made obstacles?				
7. Is exposed equipment protected against vandalism and damage?				
8. Are dumpster covers locked and dumpster area well-lighted?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-8*	*Med 9-16*	*High 17-24*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)
• Install fixed lighting to improve visibility in parking lots, entry / exit doors, and facility exterior walls - 14SW-01-LITE
• Install fixed lighting to improve visibility in parking lots, entry / exit doors, and facility exterior walls - 14SW-01-LITE
• Ensure installed lighting is placed such that it is not obstructed by man-made or natural obstacles - 14SW-01-LITE

Additional Notes / Recommendations:

VEHICLE ACCESS CONTROL & PARKING

Vehicle access and control processes can provide an important element in providing the first impression of a facility's security posture. The adequate ordering of vehicle entrance(s, parking and egress provides both long-term users and newcomers with a familiarity of structure and order that can be carried throughout a facility's environment. By offering clear site lines, stand-off distances and orderly vehicle flow and parking control, facilities can limit their exposure to general safety issues such as accidents and pedestrian strikes to more serious criminal activity, as well as reduce response times for emergency personnel should an emergency or security incident occur. In order to adequately review the facility's vehicle access control and parking, the assessor should be present during times of high vehicle and pedestrian traffic in order to completely observe and answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Does emergency vehicle access around the building meet local requirements?				
2. Are roadways through the site serpentine or otherwise indirect?				
3. Do curb lanes adjacent to building prohibit parking?				
4. Are there clear, traffic-calmed pick-up/drop-off points?				
5. Can vehicle entry beyond checkpoints be controlled, permitting entry by only one vehicle at a time?				
6. Are there perimeter barriers capable of stopping vehicles?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-6*	*Med 7-12*	*High 13-18*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Bollards or barriers should be installed to prevent vehicle based attacks and/or accidents - 14SW-01-WALL
- Bollards or barriers should be installed to clearly define pick-up and drop off points and protect pedestrians - 14SW-01-WALL
- Install vehicle and/or pedestrian gates to prevent unauthorized access and control facility grounds - 14SW-01-DOOR
- Install vehicle and or pedestrian locking devices on perimeter access points - 14SW-01-PACS

Additional Notes / Recommendations:

EXTERIOR DOORS & WINDOWS

Facility windows and doors are a key component to a defense-in-depth security approach and are a mainstay of any adequate physical security program. Secure exterior windows and doors provide for both the deterrence and delay of any criminal activity or attack. Identifying and securing/hardening exterior windows and doors should be a priority in any physical security program. Additionally, exterior windows and doors must provide not just adequate protection, but also adequate, identifiable and safe access for first responders, as well as egress for individuals in case of an emergency. In order to assess the security of the facility's exterior doors and windows, the assessor must physically observe, approach and attempt to enter/exit the individual doors and windows in order to adequately answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Other than the main entrance, are other exterior doors locked to prevent entry from the exterior?	☐	☐	☐	☐
2. Are exterior doors referenced above equipped with propped open alarms?	☐	☐	☐	☐
3. Are perimeter entryways equipped with full flush metal or solid core doors at least 1 3/4" thick and secured with deadbolt locking devices and door hinges that do not permit the pins to be removed from the exterior?	☐	☐	☐	☐
4. Are the locks on all building entry points functional and in a good state of repair?	☐	☐	☐	☐
5. Are exterior doors equipped with high quality cylindrical locks with a deadbolt at least 1" in length?	☐	☐	☐	☐
6. Are exit doors equipped with push-bars?	☐	☐	☐	☐
7. Do you designate staff to check that all doors are closed and locked at the end of the business day?	☐	☐	☐	☐
8. Are doors periodically checked for proper operation, ensuring that locks actually latch when the door is closed?	☐	☐	☐	☐
9. Are exterior doors designed to prevent unauthorized access into the building?	☐	☐	☐	☐
10. Do exterior doors have narrow windows, sidelights, fish-eye viewers or cameras to permit seeing who is on the exterior side?	☐	☐	☐	☐
11. Are windows and sidelights sized and located so that if they are broken, persons cannot reach through and open a door from the inside?	☐	☐	☐	☐
12. Are exterior doors designed and certified to resist thrown or wind-blown objects?	☐	☐	☐	☐
13. Are all exterior windows easily locked?	☐	☐	☐	☐

14. Is the glass in a door, or within 3 feet from the door lock, resistant to breaking?				
15. Do windows have security film, laminate, wire mesh, steel shutters, security drapes or other application that offers enhanced protection from debris and enhanced security?				
16. Are window hardware and frames in good condition or reinforced with slide bolts or other security devices?				
17. Are windows designed to serve as a secondary means of escape not blocked by security bars/grills, louvers, awnings, or other devices that would prevent escape?				
18. Are windows designed and located to resist the effects of gunfire and forced entry?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-18*	*Med 19-36*	*High 37-54*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- **Install reinforced doors and/or gates for increased physical security and to prevent or delay forced entry - 14SW-01-DOOR**
- **Install locking devices on facility access points to prevent unauthorized entry - 14SW-01-PACS**
- **Install access violation alarm system on exterior doors and windows to sound when left open to alert occupants - 14SW-01-ALRM**
- **Install impact resistant window film on vulnerable/accessible glass/windows to delay forced entry and injury - 14EX-00-BSIR**
- **Install impact resistant windows and/or film on vulnerable glass and windows to delay forced entry resist gunfire - 14EX-00-BSIR**
- **Install impact resistant windows and/or film on vulnerable glass and windows to mitigate blast/shock effects - 14EX-00-BSIR**

Additional Notes / Recommendations:

ACCESS CONTROL & VISITOR MANAGEMENT

Access control and visitor management refers to the efficient identification of individuals authorized to enter a facility, as well as the understanding of where they are, how long they are authorized to be there and when they are scheduled to leave. An efficient access control and visitor management program can also serve as a barrier to entry to those individuals that are not authorized to be on premises. In order to assess the facility's access control & visitor management system, the assessor must be onsite to observe the facility and visitor access process, or have significant up-to-date knowledge to answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Does the facility maintain a presence of security personnel, such as off-duty police?	☐	☐	☐	☐
2. Do visitors have to check in at an administrative office or desk before they can access other parts of the building?	☐	☐	☐	☐
3. Does visitor access allow for stand-off/remote identification?	☐	☐	☐	☐
4. Is entry granted by supervising staff, greeters, ushers or through the use of proximity cards, keys, coded entries or other devices?	☐	☐	☐	☐
5. Do all staff wear facility-issued identification credentials while on premises?	☐	☐	☐	☐
6. Do visitors require appointments?	☐	☐	☐	☐
7. Are visitors escorted at all times?	☐	☐	☐	☐
8. Are visitors asked to provide proof of identification (govt. issued) and sign in/out?	☐	☐	☐	☐
9. Are visitors provided with visitor's passes?	☐	☐	☐	☐
10. Are passes dated and designed to look different from staff identification?	☐	☐	☐	☐
11. Are visitor passes collected from visitors when they sign out?	☐	☐	☐	☐
12. Are visitors prevented from accessing unauthorized areas such as utility rooms and sensitive areas?	☐	☐	☐	☐
13. Does staff challenge or offer to assist people not wearing a visitor's pass or identification credential?	☐	☐	☐	☐
14. Are all incoming deliveries inspected before being delivered to the designated recipient?	☐	☐	☐	☐
15. Are mail/package handling procedures posted in a conspicuous location?	☐	☐	☐	☐

16. Are separate wings' buildings, doors and windows externally marked for emergency responders?				
17. Have external markings been coordinated with local first responders?				
18. Are there exit signs in all relevant languages and with simple maps or diagrams where needed to direct visitors to designated building exits?				
19. Can doors be electronically locked to block visitors' entry into the building?				
20. Have steps been taken to restrict easy access to the roof, such as ladders and other items that could be used to access the upper floors and/or rooftop of the facility secured?				
21. Are mechanical equipment enclosures on the roof protected from unauthorized access or vandalism?				
22. Is roof access from inside the building only and locked?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-22*	*Med 23-44*	*High 45-66*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- **Install & Implement a Visitor Management System for identification and processing of visitors prior to access - 14SW-01-SIDP**
- **Install & implement an Access Control System to ensure entry doors are closed and secured at all times - 14SW-01-PACS**
- **If necessary due to volume of packages and size of the facility, install package screening and inspection systems - 15SC-00-PPSS**
- **Install markings (numbers or letters) on external doors & windows and coordinate strategy with first responders - 14SW-01-PACS**
- **Install locks / access control measures to ensure access to equipment rooms, restricted areas & roof is secure - 14SW-01-PACS**

Additional Notes / Recommendations:

VIDEO SURVEILLANCE (CCTV INTERNAL & EXTERNAL

Video surveillance systems provide a method for detecting, identifying and potentially initiating responses to emergency situations. Video systems also provide a means for evidence collection and storage in the event of criminal or suspicious activity. Video systems should be both internal and external to provide efficient coverage of areas of concern to a facility to include building perimeter, building access and egress points, secure areas within the building and other sensitive areas as identified by the facility such as meeting rooms, server rooms and areas with expensive property. In order to assess the facility's video surveillance system (if applicable, the assessor must physically observe each camera and camera location, as well as the remote video images at monitoring locations in order to answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Do you have a video camera/surveillance system installed?				
2. Are the cameras actively monitored?				
3. Do the cameras cover the entrances and exits to your building?				
4. Is there video surveillance of areas adjacent to the facility?				
5. Do you have cameras covering critical areas in your business, such as server rooms or cash offices?				
6. Are images recorded offsite via web-base, retained for future use as needed and stored in a secure area?				
7. Are all of the cameras and recording devices in proper working order?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-7*	*Med 8-14*	*High 15-21*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)
•
•
•
•

Additional Notes / Recommendations:

BUILDING INTERIOR

Interior security measures provide protection from insider threats, protect critical interior systems and, for facilities with an "open door" policy, are the only line of defense between you and the public.

Interior security should be an additional layer of control working in concert with exterior security measures as part of the overall layered levels of protection. Interior security is best implemented by creating interior layers on control, restricting access to critical areas of operation and personnel (offices, executive staff, school/classrooms, etc. – public versus private spaces – as well as critical equipment. In order to review the facility's interior security posture, the assessor must physically walk the facility's interior in order to answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are all interior hallways and rooms well-lighted?				
2. Are there lockable doors or other means to secure sections of the facility when the section is not in use?				
3. Is the lockable door hardware of interior doors routinely tested to ensure doors close and lock properly, and that the door hardware is in a good state of repair?				
4. Are there locks on mechanical room doors?				
5. Is there a reinforced and alarmed storage room or closet for the secure storage of portable equipment of significant value?				
6. Are recesses, niches or blind corners visible with surveillance cameras?				
7. Are exit signs well-maintained, easily seen and pointing in the right direction?				
8. Are clear and precise emergency evacuation maps posted at critical locations and do they match their positions in the building?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-8*	*Med 9-16*	*High 17-24*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Install lighting to improve visibility in interior areas such as hallways, classrooms, and highly trafficked areas - 14SW-01-LITE
- Install lighting to improve visibility in interior areas where cameras are located to improve camera performance - 14SW-01-LITE
- Install locking devices or access control systems on interior doors to prevent unauthorized access to areas - 14SW-01-PACS
- Install access violation alarm system on sensitive doors to alert occupants when opened without authorization - 14SW-01-ALRM

Additional Notes / Recommendations:

SECURITY SYSTEMS

This section reviews the selection, application, and performance of electronic security systems. This includes the lighting, access control systems, intrusion detection systems, security camera systems, duress/panic systems, emergency phones and communications, intercom systems and applicable detection and screening systems. Reliable systems can offer front-line and immediate deterrence, detection, notification and response capabilities to any sound physical security program. In order to assess the facility's security systems (if applicable), the assessor needs to have knowledge of the system(s). This can be accomplished by physically inspecting and testing the system where applicable, as well as interacting with the company that installed and maintains the system(s).

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are panic or duress alarm buttons installed at the reception desk?				
2. Are panic alarms linked to the entire facility and EMS and routinely tested?				
3. Does the facility have an electronic intrusion detection system ("burglar alarm")?				
4. Does the alarm system cover all exterior entry points?				
5. Is the intrusion detection system armed (activated) every night?				
6. Are there clear signs and/or decals posted on the exterior of the building (doors and windows) indicating the facility is equipped with an intrusion detection system?				
7. Does the facility have a system wide emergency alert system?				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-7*	*Med 8-14*	*High 15-21*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Install panic alarms/sensors/systems, preferably carried & remotely operated as well as wall/window mounted - 14SW-01-ALRM
- Install panic alarms/sensors/systems, located at reception and/or front doors/windows to alert first responders - 14SW-01-ALRM
- If possible, install panic alarms that are linked to access control systems to lockdown the facility when activated - 14SW-01-ALRM
- Install surveillance systems, access/intrustion control system/sensors for access violations/intrusion detection - 14SW-01-ALRM

Additional Notes / Recommendations:

TRAINING & EXERCISES

Training and exercises are one of the most cost-effective measures that organizations can utilize to increase their overall security posture. Examples of training are SCN's Countering Active Threat Training (CATT), Stop the Bleed Training, and Greeter-Usher program. Adequate and recurrent training and certification in base-level security techniques and procedures is a foundational physical security posture. In order to assess the training & exercises section, the assessor should have knowledge of the facility's emergency management and training programs. These functions often reside with the facility's emergency management committee, security committee or specifically designated individual(s). The assessor should either have direct knowledge of these categories or contact the appropriate persons in order to answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are your telephones pre-programmed with emergency contact numbers?				
2. Are staff trained and have they practiced their response to handle emergencies?				
a. Nuisance phone calls				
b. Active shooter/Active assailant threat				
c. Evacuation				
d. Severe weather				
e. Suspicious bags/packages/bomb threat				
f. Fire				
g. Workplace violence				
h. Vehicle-Borne Improvised Explosive Device (VBIED)				
Totals:	0	0	0	= 0
Risk Levels:	*Low 1-9*	*Med 10-18*	*High 19-27*	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Staff/Members/Congregants & occupants of the facility should be regularly trained in Countering Active Threat Training (CATT)
- Staff/Congregants should strongly consider adopting a Greeter/Usher program to ensure the safety of its members / occupants
- Staff and members should be regularly trained in standard safety response such as AED usage, and Fire Evacuation
- Strongly consider training such as Situational Awareness, as well as full scale exercises for emergency preparedness
- Select Staff members and/or congregants should be regularly trained in Stop the Bleed procedures for life saving skills

Additional Notes / Recommendations:

POLICIES & PROCEDURES

Policies and procedures describe the methods and techniques an organization uses to maintain their security posture and are unique to each security category. Policies and procedures help to establish the process, method, order, and accountability of security programs that have been established by an organization. In order to assess the security policies and procedures section, the assessor should have knowledge of the facility's security policies and procedures program. These functions often reside with the facility's emergency management committee, security committee or specifically designated individual(s). The assessor should either have direct knowledge of these categories or contact the appropriate persons in order to answer the following questions.

Assessment Section

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Is there a single person responsible for key issuance and record keeping?	☐	☐	☐	☐
2. Are keys stored in a locked cabinet with limited, auditable access?	☐	☐	☐	☐
3. Are lost keys investigated?	☐	☐	☐	☐
4. Is valuable property engraved with an owner-applied number in a manner that permits easy identification?	☐	☐	☐	☐
5. Is there a written (preferably computerized) inventory of all property and equipment of value?	☐	☐	☐	☐
6. Are assets, equipment and items of value inventoried annually?	☐	☐	☐	☐
7. Is there a written, up-to-date child and student safety and protection policy?	☐	☐	☐	☐
8. Is there a child and youth security training program for employees and volunteers?	☐	☐	☐	☐
9. Is there a policy that requires a background check of staff and volunteers?	☐	☐	☐	☐
10. Are fingerprints taken of all facility employees who work with children?	☐	☐	☐	☐
11. Is there a policy that requires that two or more adults be present during facility-sponsored programs involving children and youth?	☐	☐	☐	☐
12. Is there a child-tag system or other child check-in and drop-off procedure?	☐	☐	☐	☐
13. Do you have a clear-desk policy for sensitive documents during non-working hours?	☐	☐	☐	☐
14. Do you have a policy requiring employees to log off, shut down and secure all computers at the end of the business day?	☐	☐	☐	☐

15. Are all your computers password-protected?				
16. Are computer passwords changed regularly?				
17. Is there an internet use policy?				
Totals:	0	0	0	= 0
Risk Levels:	Low 1-17	Med 18-34	High 35-51	

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

- Organizations should create an Emergency Operation Plan in place, and staff trained to use the plan properly
- Organizations should create a key management policy / procedure to ensure keys are tracked / adjustments made if lost
- Organizations should have background check polices in place where Early Childhood Centers are in place
- Educational institutions should create background check polices in place for all staff
- Organizations should create strong internet usage & Information technology polices to prevent intrusions and cyber attacks
- Organizations should create Access Control Polices to ensure all known & unknown persons are vetted and follow procedures
- Organizations should create and implement an Emergency Operation Plan, and train staff to use the plan properly

Additional Notes / Recommendations: