SENSITIVE INFORMATION

Security Assessment Report

School Security Assessment

School Administration
4885 Park Ridge Blvd
Boynton Beach, FL, 33426

Assessment Date: January 21, 2026
Presented by:
Secure Core LLC

1660 East Central Ave
Los Angeles, CA 90402 P. 310-413-6712
Assessor: Jessie James, Security Director

Table of Contents

BACKGROUND

Scope

On Jan. 21, 2026, Secure Core LLC, conducted a Security assessment at School Security Assessment located at the following address: 4885 Park Ridge Blvd, Boynton Beach, FL, 33426.

Based on the visual inspection conducted of the facility, surrounding property, general utilities and infrastructure, this security assessment serves to identify critical physical and procedural vulnerabilities to provide stakeholders with common mitigation solutions for consideration. The primary focus of this report is on physical security and crime prevention through environmental design. Although this report references elements regarding building safety, ADA compliance or fire hazard prevention, it is beyond the scope of this report and should be addressed respectively. The observations made by the assessor and presented in this report are based on industry standard references, best practices, acquired knowledge and the assessor's professional experience in efforts to tailor the suggested mitigation options to the physical and operational needs of the facility. Solutions for consideration listed within the report do not necessarily include every option available, but rather present some of the most common options employed within the security industry. Unless stated otherwise this security assessment does not include any aspect of IT/ Cyber vulnerabilities which should be assessed independently.

Disclaimer

Any action taken by a recipient of this report or by his/her representatives based upon this security assessment does not guarantee nor warrant in any way whatsoever that the assessed location/s, facility, its users or visitors may or may not be rendered safer, invulnerable or in any fashion impervious to successful penetration, attack or other act which could cause property damage and/or personal injury to the facility or its patrons.

By accepting this security assessment report, and or by taking or avoiding to take any action based on its written or verbal content, School Security Assessment hereby agrees to RELEASE, WAIVE, DISCHARGE, HOLD HARMLESS and NOT SUE Secure Core LLC, any of its officers and or employees, for any and all loss, harm, liability or damage caused as a consequence of the security assessment, release of the written report, pictures and assessors' opinion including any loss arising from a claim of negligence. Further, by accepting this report, School Security Assessment

agrees to INDEMNIFY Secure Core LLC, its agents, officers and employees from any loss, harm, liability, lawsuits, damages or costs, including court costs and attorney fees.

EXECUTIVE SUMMARY

Overall, the facility demonstrates a Moderate level of physical security. Critical assets are generally well protected; however, gaps in perimeter control and visitor management expose the facility to potential unauthorized access or theft.

Positive findings will be added by the assessor after review.

Key Findings

- Finding #1 - Perimeter fencing shows signs of deterioration and requires immediate attention.

- Finding #2 - Visitor management processes lack sufficient verification measures.

- Finding #3 - Surveillance camera coverage is inconsistent in key areas of the facility.

These findings represent areas where the facility's current controls may not fully align with best practices or organizational security objectives.

Recommendations

- Immediate / High Priority: Repair perimeter fencing and ensure gate locks are functional.

- Medium-Term / Moderate Priority: Implement enhanced visitor verification and escort procedures.

- Long-Term / Strategic Priority: Upgrade CCTV system for full coverage and integrate with access control.

Conclusion and Next Steps

This assessment provides a roadmap for improving physical security across the facility. Implementing the recommended measures will significantly reduce risk exposure, strengthen deterrence and detection capabilities, and improve overall resilience. It is advised that management develop an action plan assigning responsibilities, timelines, and resources to ensure timely remediation.

OSINT FOOTPRINT ANALYSIS

School Security Assessment

This report provides an OSINT threat analysis focusing on the organization and location-specific intelligence pertaining to the site at 4885 Park Ridge Blvd, Boynton Beach, FL 33426. The analysis is derived from publicly available information and aims to outline various aspects relevant to physical security.

General Organizational Intelligence

The organization operating at this location is primarily dedicated to providing educational services. Its mission emphasizes community engagement, student development, and comprehensive educational support. The organization's online presence is robust, encompassing an official website that showcases its services, mission statements, and community initiatives. Additionally, the organization maintains active social media profiles across several platforms, where it shares updates, upcoming events, and engages with the community. Known partnerships include local educational institutions and community organizations, while potential adversaries may include entities opposing educational policies or competing institutions. Past controversies involving the organization relate to budgetary concerns and allegations of misconduct that briefly attracted media attention.

Location-Specific Intelligence

The physical address of the organization is 4885 Park Ridge Blvd, Boynton Beach, FL 33426, with geographic coordinates approximating 26.5164 N latitude and 80.0916 W longitude. A review of publicly available online imagery and virtual tours reveals several significant features, including the interior layout and design of the facility. The main access points consist of multiple entrances, with designated emergency exits readily visible in virtual walkthroughs. Security measures in place appear to include surveillance cameras at key locations, electronic badge readers for controlled entry, and turnstile mechanisms at main entry points. No detailed floor plans or schematics were identified in the public domain, but protocols for emergency response and visitor access have been mentioned in publicly accessible job postings. Additionally, there are mentions of the location in real estate listings and public tenders that could expose operational details.

Leadership and Employees

Key personnel include the organization's executive team, supported by a range of administrative and operational staff. The primary figures possess LinkedIn profiles that detail their professional backgrounds, showcasing experience in education management and security roles. It is crucial to

note that there is potential exposure of their personally identifiable information (PII) online. Some members have backgrounds in law enforcement or military service, which may influence security dynamics within the organization.

Events, Routines, and Behavioral Patterns

The organization hosts various events, including community outreach programs, parent-teacher meetings, and seasonal celebrations, which could attract external attendees. Publicly available social media check-ins by employees indicate specific routines and may reveal employee schedules. There are also ongoing relationships with contractors, with regular access to the site, further contributing to established on-site patterns. Special events, especially those hosting notable figures or VIPs, warrant increased security measures and can alter the typical threat landscape.

Security and Vulnerability Indicators

The organization has engaged with external security vendors, as indicated by contracts available on public procurement sites. Complaints about existing security systems have been raised in local forums, suggesting potential weaknesses. There are no notable mentions of exposed APIs or building management systems in public discussions. However, some leaked documents were reportedly found on paste sites, offering insight into internal discussions surrounding security policies. Past incidents of vandalism have been reported, emphasizing the need for heightened awareness regarding security protocols.

Attack Surface Summary

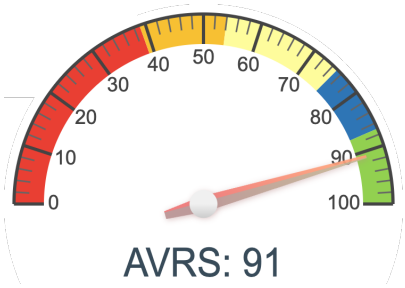
Based on the findings, potential vulnerabilities that a perpetrator could exploit include:
- Knowledge of the organizations operations and event schedules, facilitating social engineering attempts.

- Publicly accessible employee schedules and routines for crafting targeted physical infiltration strategies.

- Technical vulnerabilities that may exist within the organization's online presence or third-party contractor systems.

Overall, careful assessment of these elements aids in understanding potential attack vectors and informs the development of enhanced security measures.

QUANTITATIVE RISK ANALYSIS



Asset Vulnerability Risk Score (AVRS)

The Asset Vulnerability Risk Score (AVRS) renders a quantitative numeric ranking on the scale of 1-100, based on vulnerabilities identified and the asset's unique environmental and circumstantial factors. The higher the score, the safer the asset is.

The AVRS provides a tool to compare diverse asset variants based on unique risks identified for each. Additionally, the tool facilitates understanding risk conditions, enabling objective cross-facility comparative analysis while incorporating structural, environmental, and circumstantial variables.

The AVRS incorporates documented vulnerabilities with the assessor's chosen risk level and mitigation priorities. Additionally, the numeric result considers each security layer's importance as it pertains to the overall protection of the asset and assessment of the environmental variables, including facility type, history, operations, and current threats in the context of the real-time environment.

Definitions

Minor Risk	**88-100**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at minor risk, receiving a well above-average Asset Vulnerability Risk Score (AVRS). Few vulnerabilities were identified, which may require mitigation to enhance security.**
Low Risk	**76-87**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at low risk, receiving a slightly above-average Asset Vulnerability Risk Score (AVRS). Some vulnerabilities were identified, which require immediate attention to enhance security.**

Medium/Average Risk	**55-75**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at medium risk, receiving an average Asset Vulnerability Risk Score (AVRS). Some significant vulnerabilities were identified, which require immediate attention to enhance security.**
High Risk	**40-54**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at high risk, receiving a below-average Asset Vulnerability Risk Score (AVRS). Consequential vulnerabilities were identified in areas significant to asset security. Immediate collaborative efforts are required to improve the asset's security posture.**
Critical Risk	**0-39**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at critical risk, receiving a well below-average Asset Vulnerability Risk Score (AVRS). Consequential vulnerabilities were identified in various areas significant to asset security. Urgent collaborative efforts are required to improve the asset's security posture.**

RISK ANALYSIS AND PRIORITIZATION

The information in this section summarizes the risk level analysis determined for each vulnerability identified. The risk level was established based on professional experience and deep analysis of the threat vectors derived from the vulnerability identified, current intelligence and past incidents, probability of occurrence and the potential impact to facility structure, personnel, reputation, and operational sustainability if a vulnerability is exploited in full. Risk level definitions were set as follows:

Minor (M)

There is a very low probability of an incident occurring in which the identified vulnerability is exploited. While similar or comparable incidents may or may not have occurred in the past, there is no current evidence suggesting an imminent threat. If an incident were to take place, it may result in minor cost and/or damage to assets in addition to the possibility of minor injuries to persons, short-term operational interruption with no reputational damage.

Low (L)

There is a low probability of an incident occurring in which the identified vulnerability is exploited. Similar incidents may have occurred in the past, in the region, at comparable facility types, or at a facility with a similar vulnerability. If an incident were to take place, it may result in low cost and/or damage to assets in addition to the possibility of minor injuries to persons, short-term operational interruption with no reputational damage.

Medium (Md)

There is a moderate probability of an incident occurring in which the identified vulnerability is exploited. Similar incidents may have occurred in the past, in the region, at comparable facility types, or at a facility with a similar vulnerability. If an incident were to take place, it may result in moderate cost and/or damage to assets in addition to the possibility of severe injuries and/or loss of life, medium-term operational interruption with limited or temporary reputational damage.

High (H)

Based on threat analysis and intelligence, the probability of an incident occurring in which the identified vulnerability may be exploited is likely. Similar incidents have occurred in the recent past, in the region, at similar facility types, or at a facility with a comparable vulnerability. If an incident were to take place, it might result in significant cost and/or damage in addition to the

possibility of severe injuries and/or loss of life, long-term operational interruption with long-term significant reputational damage.

Critical (C)
Based on threat analysis and intelligence, the probability of an incident occurring in which the identified vulnerability is exploited is highly likely. Similar incidents have frequently occurred in the recent past, in the region, at similar facility types, or at a facility with a comparable vulnerability. If an incident were to take place, very significant cost and/or damage may be incurred in addition to the possibility of severe injuries and/or significant loss of life, permanent operational interruption, danger to organizational stability with long-term significant reputational damage.

Recommendations prioritizing mitigation were assigned to each vulnerability identified. Prioritization factors are based on risk severity, the assessed threat, the potential impact on the facility and personnel, the estimated resources available, and the urgency to take remedial action:

Accept (Ac)
Identified risks have been evaluated as acceptable or tolerable. No further remedial actions are required at this time. Re-evaluation is required periodically, or in the case new information becomes available.

Transfer (Tr)
Risk should be transferred to a third party, including but not limited to an insurance provider, release, waiver, or official documentation.

Mitigate C (MC)
The identified vulnerability and associated risk should be re-evaluated periodically. Remediation should take place in the foreseeable future, when time and/or resources become available.

Mitigate B (MB)
The identified vulnerability and associated risk should be remediated as soon as time and/or resources become available.

Mitigate A (MA)
The identified vulnerability and associated risk are of the highest priority and should be

remediated immediately. Temporary solutions may be applied until the vulnerability and risk are sufficiently addressed.

RISK LEVEL	SECTION	AREA	VULNERABILITY	PRIORITY
High	Perimeter	Fence	Deficient Perimeter Fence/Wall	Mitigate A
High	Building	Emergency Exit	Rapid Egress Denial- Fire Hazard	Mitigate A
High	Interior	Classroom 19A	Insufficient Access Control	Mitigate A
High	Equipment	Emergency "Go" Bag	Deficient Emergency Equipment	Mitigate A
Medium	Perimeter	Parking Lot	Insufficient Lighting	Mitigate B
Medium	Building	Building Frontage	Excessive Access Points	Mitigate B
Medium	Interior	Classroom 23B	Enables Interior Surveillance	Mitigate A
Medium	Procedures	Accountability & Missing Student/Staff	Insufficient Procedure	Mitigate A
Medium	Procedures	Lock-Down Plan	Undesignated Cover and Concealment Areas	Mitigate A
Low	Perimeter	Parking Lot	Vehicular Impact	Mitigate C
Low	Building	Building Frontage	Structural Weakness/Unprotected Glass	Mitigate C

PERIMETER

Fence

MA H

Vulnerability: Deficient Perimeter Fence/Wall

The facility is not enclosed within a perimeter boundary such as a fence or wall. The existing perimeter is insufficient and will not prevent an intruder from accessing exclusive areas.

Recommendations

- **Anti-Climb Fencing**

Install an anti-climb fence or wall. Different styles of anti-climb fencing are available, most consisting of vertical bars with horizontal supports designed to

make scaling difficult. Additional measures may include appropriate lighting, security cameras, alarm devices, and signage to augment the perimeter boundary.

Reference: FEMA 426, 2-25

- **Fencing/Wall Enclosure**

Install a perimeter fence or wall enclosing the facility within a physical boundary. Fencing types include but are not limited to chain-link, aluminum, anti-climb (CPTED), barbed wire, concertina, triple-stranded concertina, welded mesh, buried fencing, wrought iron, and wire, all of which are designed to deter and delay intrusion. Additional measures may include appropriate lighting, security cameras, alarm devices, and signage to augment the perimeter boundary.

Reference: FEMA 426, 2-53

- **Security Signage**

Post security signage along the facility's perimeter to deter possible unlawful activity and to establish territoriality. Include wording such as, "No Trespassing" or "Under CCTV Surveillance." As a deterrent, proper signage can advise personnel of select security systems employed on the property. Signage should be concise, legible from a distance, well lit, and printed in all relevant languages.

Reference: ASIS-Physical Security, P. 85, FEMA 428, F-3, FEMA 426, 2-70, 5-29

- **Security Camera Installation**

Install security camera/s to monitor activity around the facility perimeter. Sufficient security camera coverage may substitute the need for frequent patrols to the area. The camera type/model installed should suit lighting and weather conditions, day and night. For increased deterrence, install cameras in overt locations, strategically placed to avoid vandalism, sabotage, or environmental damage. Motion activated security camera sensors may also be used to detect and alert of any movement or intrusion attempt in the area.

Reference: FEMA 426, 2-29, 4-21, 5-44, ASIS-Physical Security, P. 103

Parking Lot

MB Md

Vulnerability: Insufficient Lighting

There is insufficient lighting in the parking lot. Inadequate lighting creates general safety hazards and may promote unlawful activity in the area. Additionally, limited lighting may render existing surveillance equipment ineffective.

Recommendations

- **Illumination Quality Upgrade**

Upgrade the current parking lot light bulbs and/or luminaires for better illumination capabilities. Different light sources have different abilities and limitations. When choosing the optimum light source, various factors should be considered, such as the threat level, cost of change and usage, life usage expectancy (in hours), accessibility, maintenance, environment, and design

Reference: ASIS-Physical Security , P. 71, P.169-185

- **Standby Lighting**

Where continuous lighting is not required, install standby lighting within the parking lot. Standby lighting activates when motion is detected by the sensor.

Reference: FEMA 426, 2-68

MC L

Vulnerability: Vehicular Impact

Both the facility's exterior and pedestrians in the parking lot are vulnerable to vehicular impact. Injuries and/or structural damage may occur due to an accidental or intentional vehicular incident.

Recommendations

- **Planter Placement**

Place planters in strategic locations in and around the parking lot. Planters should be anchored and filled with weighted material to prevent displacement in the event of a collision. Ensure planters installed do not interfere with routine operations, visibility, or emergency response access.

Reference: FEMA 426, 2-45, B-21

- **Traffic Regulatory Signage**

Post regulatory traffic signage in and around the parking lot to remind drivers of traffic flow and vehicle speed regulations. Ensure crosswalks, waiting areas, and high-risk areas are appropriately marked to inform passing motorists.

Reference: FEMA 426, 2-70

- **Bollard Installation**

Install bollards along vulnerable areas in the parking lot. Bollard size and depth are determined by the vehicular threat level and should typically not exceed 30 inches in height. Bollard spacing should be between 36 to 48 inches (0.9 and 1.2 meters), comply with ADA regulations, and facilitate emergency response access.

Reference: FEMA 426, 1-41, 2-20, 2-37, 2-42

BUILDING

Building Frontage

MB Md

Vulnerability: Excessive Access Points

There are multiple access points along the building frontage providing access to the facility. An excess number of access points can make the facility more susceptible to unauthorized entry. Multiple access points are difficult to monitor and make proper access control challenging. Additionally, efforts to secure the facility in a lockdown may be delayed.

Recommendations

- **Access Point Minimization**

Depending on security resources available, access using entry points along the building frontage should be limited to one single entry point, where visitors can be screened appropriately before entering the facility. Alternate access points may serve as exits or entryways for credentialed staff and authorized personnel. Preferably, alternative entrance points should be equipped with remote monitoring, intrusion detection, and designed to prevent entry of unauthorized personnel.

Reference: FEMA 426, 1-40, APTA SS-SIS-S-010-13, Rev. 1, P.26

MC L

Vulnerability: Structural Weakness/Unprotected Glass

The material or design of the building frontage is not resilient and may be vulnerable to damage or intrusion. Materials such as unprotected glass and hollow wood increase the risk of potential intrusion, damage to the facility, or injury to personnel. In an explosion, lite materials such as glass and wood may be projected into the facility at high speed, resulting in injury or damage.

Recommendations

- **Glass Protection Film**

Treat the unprotected glass along the building frontage with shatter resistant, fragment retention, tinted and anchored protective security film. While the security film may limit glass fragmentation and delay an intrusion, the tinting will provide additional privacy screening so an aggressor cannot easily see inside the building.

Reference: FEMA 426, 1-35, 3-73

Emergency Exit

MA H

Vulnerability: Rapid Egress Denial- Fire Hazard

The emergency exit door/gate may violate fire code, potentially restricting or delaying emergency egress of facility occupants. A malfunctioning lock, improperly installed locking device or blocked route may result in delayed and disorderly evacuation in case of an emergency.

Recommendations

- **Egress Pathway Clearance**

Ensure the area leading to and around the emergency exit is clear of debris and clutter to facilitate quick evacuation in case of an emergency.

Reference: NYPD Engineering Security Protective Design for High Risk Buildings, Pg. 62

- **Crash Bar Installation**

Install a crash bar on the emergency exit's interior, which quickly unlocks when pressure is applied in the direction of egress. Ensure a door spring is installed to prevent the door from remaining open after use.

Reference: FEMA 426, B-7

INTERIOR

Classroom 23B

MA Md

Vulnerability: Enables Interior Surveillance

The arrangement and design of the classroom enables outside observation into the room. Although the configuration may facilitate a positive study environment, observation allows an aggressor to collect valuable information on occupants and

security measures. Additionally, the design limits the number of locations affording sufficient concealment for staff and students.

Recommendations

- **Tinted Glass Film**

Install sufficient window tinting or frosting film on the classroom windows to restrict outside observation into the room. Window tinting is particularly effective when interior lighting is turned off.

Reference: FEMA 426, F-8

- **Curtains/Shades Installation**

Furnish pertinent windows with curtains or shades in the classroom to ensure interior activity cannot be viewed from outside the room in an emergency.

Classroom 19A

MA H

Vulnerability: Insufficient Access Control

Access to the classroom is not adequately controlled through one or more of its entrances. School equipment, sensitive information, property or personnel may be at risk. In the case of an incident, the ability to conduct a proper post-incident investigation is limited.

Recommendations

- **Entrance Door Repair/Replacement**

Repair/replace the classroom entrance door, ensuring it properly seats when closed and locks securely in place.

Reference: FEMA 459, 5-5

EQUIPMENT

Emergency "Go" Bag

MA H

Vulnerability: Deficient Emergency Equipment

The classroom emergency "Go" bags are missing key items. Occupants will not have access to critical supplies in case of an emergency evacuation.

Recommendations

- **Periodic Inventory Inspection**

Periodically inspect and inventory emergency bags to ensure readiness and compliance. Inventory checks should be documented and expired medical supplies should be removed and replaced.

PROCEDURES

Accountability & Missing Student/Staff

MA Md

Vulnerability: Insufficient Procedure

The organization does not have a procedure to efficiently monitor and manage student/staff accountability at all times, both on and off-site. Protocols should

include actions in the case of a missing student or staff member. Deficient procedures can delay emergency response/involvement and may result in physical harm and/or liability.

Recommendations

- **Accountability & Missing Student/Staff Procedures**

Ensure proper procedures and systems are in place to detect, inform and take appropriate actions in the case of a missing student or staff member. Ensure full accountability at all times while on the premises. Additionally, procedures should be established to identify and investigate suspicious absences to promptly address any security, safety or behavioral concerns.

Lock-Down Plan

MA Md

Vulnerability: Undesignated Cover and Concealment Areas

The current facility lock-down plan does not define or designate cover and concealment areas within each safe room/haven. In the case of a lock-down situation, unestablished or inaccessible cover and concealment locations may prompt occupants to seek refuge in unsuitable areas.

Recommendations

- **Defined Cover and Concealment Area**

Designate and define optimal cover and/or concealment locations within each safe room/haven for occupant consideration in case of a lockdown. Designated cover and concealment areas within each secure room should be clearly identified and marked to ensure a quick and effective response during an emergency. Facility users should be aware of what differentiates cover and concealment as it directly impacts protection levels in the case of a lock-down.

REFERENCES

1. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings - FEMA-426/BIPS-06/October 2011, Edition 2*
2. *U.S. Department of Veterans Affairs, Physical Security and Resiliency Design Manual, October 1, 2020 , Revised May 1, 2024*
3. *Taking Shelter from the Storm: Building or Installing a Safe Room for Your Home, Includes Design Plans-FEMA P-320, December 2024, Sixth Edition*
4. *Guide for Developing High-Quality School Emergency Operations Plans - US Department of Education, June 2013*
5. *Safe Rooms for Tornadoes and Hurricanes-Guidance for Community and Residential Safe rooms- FEMA P-361, November 2024 Fifth Edition, Second Issuance*
6. *Physical Security for Public Transit - APTA Standards Development Program - Recommended Practice - American Public Transportation Association- SS-SIS-S-010-13, Rev. 1, May 23, 2023*
7. *Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings-FEMA-428/BIPS-07/January 2012, Edition 2*
8. *A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings FEMA 452 / January 2005*
9. *Incremental Protection for Existing Commercial Buildings from Terrorist Attack Providing Protection to People and Buildings- FEMA 459 / April 2008*
10. *Manual of Security Policies and Procedures - US Department of Commerce -29-May-2017*
11. *New York Police Department, Engineering Security, Protective Design for High Risk Buildings - 2009 Edition*
12. *Design Guidance for Shelters and Safe Rooms- FEMA 453 / May 2006*
13. *DHS Bomb Threat Checklist- https://www.cisa.gov/resources-tools/resources/bomb-threat-checklist*
14. *Earthquake Safety Checklist- FEMA B-526 / October 2023*
15. *2016 DHS-DOJ Bomb Threat Guidance Brochure - https://www.dhs.gov/sites/default/files/2024-12/24_1205_fps_bomb-threat-procedures-card-508.pdf*
16. *FEMA: Parent-Student Reunification Procedures (from Washington Military Department's Emergency Management Division), April 2011*
17. *Fire/Emergency Medical Services Department Operational Considerations and Guide for Active Shooter and Mass Casualty Incidents, 2013*
18. *FEMA - IT Disaster Recovery Plan: https://www.ready.gov/business/emergency-plans/recovery-plan*
19. *FEMA: Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, May 2025, Version 3.1*
20. *DHS:US Secret Service: Enhancing School Safety Using A Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence , 2018,*

https://www.secretservice.gov/sites/default/files/reports/2020-10/USSS_NTAC_Enhancing_School_Safety_Guide.pdf

21. *Severe Weather Planning for Schools, National Clearinghouse for Educational Facilities, 2008, https://files.eric.ed.gov/fulltext/ED539488.pdf*
22. *Design Guide for Improving Critical Facility Safety from Flooding and High Winds-FEMA 543 / January 2007*
23. *National Incident Management System (NIMS), Department of Homeland Security, December 2008*
24. *A Resource Guide to Improve Your Community's Awareness and Reporting of Suspicious Activity/ FEMA P-904/ February 2012*
25. *ASIS International - Protection of Assets, Physical Security, 2012*
26. *Center For Disease Control and Prevention (CDC)- Coronavirus disease 2019- https://www.cdc.gov/coronavirus/2019-nCoV/index.html*
27. *World Health Organization - Novel-Coronavirus-2019- https://www.who.int/emergencies/diseases/novel-coronavirus-2019*
28. *US Department of Labor- Occupational Safety and Health Administration-OSHA 3990-03 2020*