Ohio™ Department of Higher Education

HigherEd.Ohio.gov

Mike DeWine, *Governor* Jon Husted, *Lt. Governor* Mike Duffey, *Chancellor*

Campus Security Support Program Grant Request for Proposals (RFP)
Release Date: December 2, 2024
Submission Date: January 31, 2025 at 12:00 p.m.

Program Purpose

To support Ohio institutions of higher education as they work to foster a safe, inclusive, and respectful education environment, the Ohio Department of Higher Education ("ODHE"), per Section 381.220 of Amended Substitute Senate Bill 94 of the 135th General Assembly, was charged with developing the guidelines and procedures to apply for funding through the *Campus Security Support Program Grant*.

Through the *Campus Security Support Program Grant*, ODHE seeks proposals from institutionally sanctioned student organizations at Ohio colleges and universities who are affiliated with communities that are at risk for increased threats of violent crime, terror attacks, hate crimes, or harassment to enhance security measures and increase student safety.

Eligible Applicants

Eligible applicants include state institutions of higher education and private nonprofit institutions of higher education that have institutionally sanctioned student organizations.

The following institution types are eligible:

"State university" means a public institution of higher education that is a body politic and corporate. Each of the following institutions of higher education shall be recognized as a state university: University of Akron, Bowling Green State University, Central State University, University of Cincinnati, Cleveland State University, Kent State University, Miami University, Northeast Ohio Medical University, Ohio University, Ohio State University, Shawnee State University, University of Toledo, Wright State University, and Youngstown State University.

"State institution of higher education" means any state university or college as defined in division (A)(1) of section 3345.12 of the Revised Code, community college, state community college, university branch established under Chapter 3355. of the Revised Code, or technical college.

"Private college" means any of the following:

(1) A nonprofit institution holding a certificate of authorization pursuant to Chapter 1713. of the Revised Code;

(2) An institution holding a certificate of registration from the state board of career colleges and schools and program authorization for an associate or bachelor's degree program issued under section 3332.05 of the Revised Code;

(3) A private institution exempt from regulation under Chapter 3332. of the Revised Code as prescribed in section 3333.046 of the Revised Code.

For the purposes of this RFP, ODHE defines "an institutionally sanctioned student organization" as an organization recognized by, or operating under, the sanction of an institution according to the individual institution's student organization recognition process. At a minimum the student organization must:

- Be created or established for a purpose which supports the sponsoring institution's mission, goals, and vision.

- Majority of membership is verified by the institution to be currently enrolled undergraduate and/or graduate students at the sponsoring institution.
- Has advisory oversight in some capacity from the sponsoring institution (ex. faculty advisor, student activities/development office representative, or similar).
- The organization has some form of institutionally verified organizational and operational structure.

This definition was created for this RFP and award process only and should not be construed as the definition for other purposes on campus or under other ODHE programs. Potential applicants should consult with their institution's legal counsel in determining if they meet the definition of an "institutionally sanctioned student organization" is met for purposes of this RFP and to confirm the institution will provide the required certification.

I. Anticipated Awards

The total of all awards under the *Campus Security Support Program Grant* will not exceed the total funding available. The Chancellor is not obligated to expend all funds set aside for this initiative and may request revisions to proposal budgets.

1. Total Award Funding Available: up to $1,900,000.00
2. Maximum Base Award per Institution: $50,000 per proposal

II. Eligible Expenses and Project Term

Institutionally sanctioned student organizations seeking funding through the *Campus Security Support Program Grant* should submit proposals that identify how the funds will help to mitigate risks for increased threats of violent crimes, terror attacks, hate crimes, or harassment to enhance security measures and increase student safety at institutions of higher education.

Funding requests for physical security and safety of a building owned, or leased for the next 5 years, by the institutionally sanctioned student organization, or their sponsoring organization, will require a security vulnerability assessment (SVA) which has been conducted and submitted for each building or location requesting funding for security improvements. Each applicant must include its SVA and describe how the award will be used to address the vulnerabilities identified in the assessment. The SVA should be conducted by experienced security, law enforcement or military personnel. The completed SVA must be submitted separately from the application to schoolsafetygrants@dps.ohio.gov. SVA can be accessed at https://rfp.ohiohighered.org/.

Funding may be used to hire additional security for an event, program and/or speaker. The security provider must be licensed by the Private Investigator Security Guard Services (PISGS), a component of the Ohio Homeland Security, and if the provider is not employed by the institution for other safety and security related functions the security organization is responsible for establishing a formal agreement with the institution's campus police or security entity.

Private Investigator Security Guard Services | Ohio Homeland Security

Funds may not be used to purchase weapons for the institutionally sanctioned student organization or any of its members. This would include not being able to purchase firearms, ammunition, or any less than lethal components. Less than lethal components would include pepper spray, batons, or similar products.

Campus Security Support Program Grant proposals that are awarded funds through this RFP will have through June 30, 2025, to complete the scope of work for the program, beginning when an agreement is executed between ODHE and the institution. Planning may commence upon acceptance of the grant award notification.

A final program and expense report will be due from the institution 30 days after the end of the expenditure period. An interim report detailing progress on specific components of the proposed initiative, including milestones achieved, expenses, and evaluations will need to be submitted by mid-March 2025. Additional information will be set forth in the grant agreement. Reports should be sent to the ODHE safety grants team, ODHEsafetygrants@highered.ohio.gov.

III. Proposals Review Process and Timeline

The schedule below may be revised by the Chancellor, at the discretion of the Chancellor. Any changes will be communicated to applicants.

Request for Proposals Released	December 2, 2024
Proposal Questions from Interested Parties	December 5 – December 13, 2024
Proposals Due by 12:00 p.m.	January 31, 2025
Proposal Review Period	February 3 – February 21, 2025
Notification of Awarded Proposals	Week of February 24, 2025

The Chancellor will provide information to interested parties and provide assistance to potential applicants by responding to questions submitted via e-mail to: ODHEsafetygrants@highered.ohio.gov by the deadline.

Questions must be submitted by December 13, 2024, to ensure an answer by December 20, 2024. Responses will be posted at https://rfp.ohiohighered.org/

The Chancellor's staff will initially screen proposals for completeness and eligibility. Any deficiencies must be addressed by the applicant within a time period set by the Chancellor's staff. While all properly submitted proposals will receive consideration, submission of a complete proposal does not guarantee funding.

Upon applicant approval, the Chancellor will provide an award notification letter to the institution, which will include the total awarded amount. ODHE and the applicant will enter into an agreement prior to funding being disbursed.

IV. Proposal Submission

Applicants are responsible for submissions of proposals within the time period set by the Chancellor. Proposals must include the address for the institution where funds awarded may be sent. This address needs to be registered in the Ohio Pays system. Proposals must be received no later than 12:00 p.m. on January 31, 2025, and must be submitted in the following manner:

> One electronic PDF file that includes: the cover letter, executive summary, project narrative, and the budget narrative and budget using the provided spreadsheet template, emailed to the ODHE safety grants team at ODHEsafetygrants@highered.ohio.gov.

Funding requests for physical security and safety of a building owned, or leased for the next 5 years, by the institutionally sanctioned student organization, or their sponsoring organization, must submit their completed Security Vulnerability Assessment separately. The SVA should go to schoolsafetygrants@dps.ohio.gov. Only the completed SVA should be sent to this email address. **Do not send the SVA to ODHE for security reasons.** However, please indicate on your application that the SVA has been submitted to the Ohio School Safety Center via the email address provided.

All information submitted in response to this RFP is public information unless a statutory exception exists that exempts it from public release under the Ohio Public Records Act in Section 149.43 of the Ohio Revised Code.

V. Proposal Requirements

A. Format

Proposals must be submitted in Arial Font, 11 point and double-spaced; there is an exception for tables and images, where the font may be single spaced. Please see below for page allocations and directions for each section of the proposal.

1. **Cover Letter (one page maximum):**
   a. Title of project,
   b. Names of the institutionally sanctioned student organizations.
   c. Primary contact from each institutionally sanctioned student organization by name, student organization and title within the organization, and email address,
   d. Primary institutional contact (from the institution receiving the funds) by name, title, address, phone number, and email address,
   e. Total amount of funding being requested.

2. **Executive Summary (two pages maximum):** Provide a description of the security needs to be supported by the proposal, including clearly identifying the institutionally sanctioned student organization(s) to be supported, and the specific security concern the funds seek to address. The applicant should provide supportive data, specific to the local student organization(s), which demonstrates the security concern and/or threat, where applicable.

3. **Project Narrative (ten pages maximum):** The project narrative should address the Proposal Criteria in order (see Section C). Depending on the request, additional documentation may be required (see project rationale below). That documentation does not count toward the 10-page maximum limit.

4. **Budget and Budget Narrative:** In the provided Excel spreadsheet, the budget and budget narrative will document:
   a. Itemized costs for the grant
   b. The underlying assumption for each cost (i.e., base cost of the item or service, how it ties to the overall outcomes associated with the proposal, and number of persons involved/served, etc.)
   c. Any matching funds that will be leveraged, clearly labeled.

5. **Certification Letter**: A letter from the appropriate Vice President or equivalent at the institution where the sanctioned student organizations are located must be submitted with the proposal. The letter must certify that the student organizations applying for funding are institutionally sanctioned, at a minimum by the ODHE definition provided in this proposal, and that the institution is prepared to support the student organization with all grant accounting and reporting requirements which will be set forth in the award agreement if funds are awarded.

6. **Security Vulnerability Assessment**: Funding requests for physical security and safety of a building owned, or leased for the next 5 years, by the institutionally sanctioned student organization, or their sponsoring organization, will require a Security Vulnerability Assessment (SVA) which has been conducted and submitted for each building or location requesting funding for security improvements. Each applicant must include its SVA and describe how the award will be used to address the vulnerabilities identified in the assessment. The SVA should be conducted by experienced security, law enforcement or military personnel. The completed SVA must be submitted separately from the application to schoolsafetygrants@dps.ohio.gov. **Do not submit the SVA to ODHE with the application for security reasons.** However, please indicate on your application that the SVA has been submitted to the Ohio School Safety Center via the email address provided.

B. Scoring Rubric

Each proposal will be assessed according to the proposal criteria:

• Project Design	20 points
• Project Rationale	30 points
• Project Plan	20 points
• Budget & Budget Narrative	10 points

C. Proposal Criteria

Project Narratives are required to address the following:

i. Project Design: Broad description of the perceived, anticipated and/or demonstrated threats of violent crime, terror attacks, hate crimes, or harassment towards institutionally sanctioned student organization(s) for affiliated communities at risk for such incidents to be addressed through the awarded grant funds.

This section should include an overview of:

a. The institutionally sanctioned student organization(s) and the communities affiliated with the organization(s) which are at risk, including any local examples of real or perceived threats to the organization and how the funds will be used to mitigate those threats.

b. The specific issues or concerns the funds are seeking to address and how they have been identified.

c. A summary regarding the current relationship between the institutionally sanctioned student organization(s) and the campus police and/or security with respect to the identified security issue or concern. If non-campus law enforcement (ex. municipal police, sheriff) is also engaged with the student organization(s) please include that information as well.

d. Information about the relationship between the student organization(s) and other campus offices and/or administrators who have also been providing oversight or support for the security concerns outlined in the proposal.

ii. Project Rationale: Detailed description, including:

a. Detailed description as to how the funds will be used.

b. Rationale that explains how the proposed security improvements will seek to mitigate the threats to the institutionally sanctioned student organization(s).

c. Identify short-term and long-term impact of the proposed security improvements for the institutionally sanctioned student organization(s).

d. Please provide information as to the current relationship between the institutionally sanctioned student organization(s) and the campus police and/or security, including the campus police and/or security entity's understanding of and/or involvement in the security improvements being sought through this grant program.

e. If the institutionally sanctioned student organization(s) is seeking to partner with an external security provider for an event, program and/or meeting, please detail how the security provider was identified and their current relationship with the campus police and/or security at the institution. A copy of the security provider's Private Investigator Security Guard Services (PISGS) license must be provided with the application.

f. If the institutionally sanctioned student organization is requesting funds to support security improvements to their physical structure, a copy of the completed security checklist must be submitted with the proposal. The student organization should also provide documentation demonstrating ownership of the property or a lease agreement for the property through 2030. These documents do not count against the total pages allowed for the Project Narrative.

iii. Project Plan: This section will provide a clear description and timeline for activities to be undertaken.

a. Outline the roles and responsibilities of key partners.

b. Shared goals and outcomes established by the campus partners to guide the work to be completed with the grant funding.

c. Timeline for milestones and planned activities for the proposed project including a detailed narrative with key partners and intended activities for each milestone listed. Please also indicate if it is anticipated that the milestone will use grant funds to achieve.

d. Provide the name, email, and phone number for at least two administrative leaders for the project.

i. Both individuals must be employees of the college/university where the student organizations are institutionally sanctioned. One of the administrative leaders must be a representative from the grants or sponsored programs office at the institution receiving the funds. The other leader must be a representative from student development or the institutional division which sanctions student organizations.

ii. One of the individuals can be the same person as the primary contact listed on the cover page.

D. Budget Narrative

1. The amounts for each budget line activity must be documented and justified in the budget narrative and summarized within the provided Excel workbook.
2. The narrative should include an estimate as to the timing of expenditures in relation to the project plan.
3. Costs should fall within comparative industry standards.

VI. Legal Notices

The applicant understands that if its application is accepted by the State, the applicant shall enter into an agreement with the State governing the use of the awarded funds. The applicant agrees to comply with all applicable federal, state, and local laws and regulations in the conduct of the work hereunder.

The State reserves the right to fund any application in full or in part, to request additional information to assist in the review process, to require new applications from interested parties, to reject any or all applications responding to this announcement, or to reissue the announcement if it is determined that it is in the best interest of the State of Ohio. Issuing this announcement does not bind the State to making any awards. The State reserves the right to adjust the dates for this announcement for whatever reasons are deemed appropriate. The State reserves the right to waive any non-substantive infractions made by an applicant, provided that the applicant cures such infraction upon request.

All costs incurred in preparation of an application shall be borne by the applicant. Application preparation costs are not recoverable under an award. The State of Ohio shall not contribute in any way to recovering the costs of application preparation.

The funding decisions are final. Applicants will be notified of the outcome of their application(s) at the conclusion of the review process.

The applicant understands that the information provided herein is intended solely to assist the applicant in submittal preparation. To the best of the State's knowledge, the information provided is accurate. However, the State does not warrant such accuracy, and any errors or omissions subsequently determined will not be construed as a basis for invalidating this solicitation. Interested parties bear the sole responsibility of obtaining the necessary information to submit a qualifying application. The State retains the right to modify or withdraw this solicitation at any time. By submitting an application, applicants expressly agree to these terms.

VII. <u>Trade Secrets</u>

All Applicants are strongly discouraged from including in a proposal any information that the Applicant considers to be a “trade secret,” as that term is defined in Section 1333.61(D) of the Ohio Revised Code.

1. To determine what qualifies as trade secret information, refer to the definition of “trade secret” in the Ohio Revised Code at 1333.61(D), which is reproduced below for reference:

   > “(D) ‘Trade Secret’ means information, including the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, pattern, compilation, program, device, method, technique or improvement, or any business information or plans, financial information, or listing of names, addresses, or telephone numbers that satisfies both of the following:
   >
   > (1) It derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
   >
   > (2) It is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

2. If any information in the proposal is to be treated as a trade secret, the proposal must:

   a. Identify each and every occurrence of the information within the proposal with an asterisk before and after each line containing trade secret information and underline the trade secret information itself;

   b. Identify that the proposal contains trade secret information in the cover letter; and

   c. Include a summary page immediately after the cover letter that lists each page in the proposal that includes trade secret information and the number of occurrences of trade secret information on that page.

3. The Ohio Department of Higher Education requires non-disclosure agreements from all non-Department of Higher Education persons who may have access to proposals containing trade secret information, including evaluators.

4. If the Applicant claims that a record is not subject to disclosure under the Ohio Public Records law based on trade secret, it will bear costs of defending this claim.

Ohio™ School Safety Center

What is a Security and Vulnerability Assessment (SVA)?

The process of defining, identifying, classifying, and prioritizing vulnerabilities that are specific to a physical location and recommending areas of improvement.

The goal of conducting one of these assessments is to identify gaps and mitigate soft targets for the requesting agency and to provide a comprehensive review of trends for physical safety and security.

Some baseline security categories typically assessed include:

- Mass Notification
- Intrusion Detection
- Visitor Procedures
- Key Control Procedures
- Access Control
- Video Surveillance
- Lighting around property

To identify vulnerabilities, schools both K-12 and Higher Education will work with their local law enforcement, military personnel or security professionals experienced in conducting SVAs to complete a vulnerability assessment developed by the Ohio Homeland Security. More details on the tool will be included with the grant solicitation.

These assessments will direct schools in a step-by-step process to determine their vulnerabilities. The person conducting the assessment will review any areas of improvement as well as some options for consideration with the applicant.

These options may include updates to procedures and practices (no cost) or even suggested physical security upgrades (for purchase) and are tailored based on the individual facility's vulnerabilities. These reports can then be used to justify budget requests and apply for state and federal grant opportunities.

The report is protected by ORC 149.433 and should not be disseminated to those without a need-to-know or right-to-know.

Vulnerability Assessment

Campus Security Support Program Grant S.B. 94

Please note: Prior vulnerability assessments conducted by experienced security (including Ohio Homeland Security), law enforcement, or military personnel, may be used if they were conducted on or after January 1, 2023. If a previous assessment from this time period is used, it must be attached with the submission and this form still must be filled out using the previous assessment.

Instructions for completing the Vulnerability Assessment

1 - Report population at **peak attendance** (maximum capacity).

> Example: The facility has a population of around 150 that meets regularly throughout the year. The facility also hosts (2) short-term, special events during the year that have an attendance of up to 750. The population should be reported, at its peak, of 750.

2 - Report **vulnerabilities** at the weakest part of the asset.

> Example: The property is surrounded by a fence that is completely intact and has 5 openings; 4 openings have gates and one opening is unsecured. In this case, the weakest component of the fence system is the unsecured opening and the entire asset would be considered unsecured.

3 - Attach an **aerial map** showing the perimeter and layout around the site.

4 - Submit this assessment electronically with other application documents to: schoolsafetygrants@dps.ohio.gov.

Name of individual conducting assessment: ___________________________________

Title of person conducting assessment: _______________________________________

Experienced Security/Law Enforcement/Military: _____________________________

Answer each question below. (Responses to questions that are partially 'yes' or partially 'no' should be considered as 'no.')

FACILITY INFORMATION

1. In which city is the facility located?

   □ _________________________

2. What is the maximum facility population at any one time?

   □ _________________________

3. Does this asset have a significant symbolic and/or psychological impact?

   □ Symbolic
   □ Psychological

FACILITY THREATS AND HAZARDS

1. Has the facility been free of vandalism within the past five (5) years?

   □ No

   a. Describe: ________________________________

   □ Yes

2. Has the facility been free of any threats within the past five (5) years?

   □ No

   a. Describe: ________________________________

   □ Yes

FACILITY OPERATIONS

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #3, #4, #67, #68, #77, #78, #79 and #84. Any additional items must be justified within the application.

1. Are events from external sources prohibited? (i.e., community events, recreational activities, meetings, private gatherings such as weddings and family reunions)

   □ No

   □ Yes

2. Does the facility assign personnel to monitor activities (i.e., beginning/end of business day, passing periods, and after-hours events)?

   □ No

   □ Yes

POLICY AND PROCEDURE MANUALS

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #75, #76 and #79. Any additional items must be justified within the application.

1. Does the facility have a written Emergency Operation/ Emergency Action Plan?

   □ No

   □ Yes

2. Does the facility have a written security policy?

   □ No

   □ Yes

3. Is the security policy regularly reviewed and updated?

   □ No

   □ Yes

4. Are safety drills conducted?

   □ No

   □ Yes

5. Does the facility hold active aggressor training?
   - □ No
   - □ Yes
6. Does the facility have a system / procedures in place for lockdowns?
   - □ No
   - □ Yes
7. Are staff (and, if applicable, security personnel) adequately trained on how to activate the lockdown system?
   - □ No
   - □ Yes

BAG CHECK POLICY

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: : #3, #66, #68 #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is a written bag policy in place?
   - □ No
   - □ Yes
2. Does the facility have policies for conducting searches for weapons, drugs, and other contraband?
   - □ No
   - □ Yes

FIRST RESPONDERS

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #75, #79 and #83. Any additional items must be justified within the application.

1. Have local first responders toured the facility?
   - □ No
   - □ Yes
2. Is there a method for emergency responders to gain access to the facility after business hours?
   - □ No
   - □ Yes

INFORMATION SHARING

1. Does the facility exchange security and threat information with external agencies?
   - □ No
   - □ Yes
2. Have floor plans and site plans been provided to first responders?
   - □ No
   - □ Yes

MASS NOTIFICATION SYSTEM / EMERGENCY COMMUNICATIONS

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #2, #29, #30, #32, #46, #61, #69, #76, #77, #78, and #79. Any additional items must be justified within the application.

1. Is a functioning public address system in place that allows the office (or central location) to communicate to the whole facility?
   - □ No
   - □ Yes
2. Is the staff trained to use the Public Address (PA) and or duress system?
   - □ No
   - □ Yes
3. Is there a public address system that can be heard outside the building?
   - □ No
   - □ Yes
4. Are all rooms able to communicate with the command center, front office, first responders, etc.?
   - □ No
   - □ Yes
5. Does the phone system allow a 911 call to be placed without entering a passcode or dialing for an outside line (E911 system)?
   - □ No
   - □ Yes
6. Are the facility's telephones pre-programmed with emergency contact numbers?
   - □ No
   - □ Yes
7. Is a "duress" system or panic button available in the office that alerts law enforcement?
   - □ No
   - □ Yes
8. Does the "duress" system or panic buttons alert security personnel in the security control room?
   - □ No
   - □ Yes
9. Is the "duress" system or panic button available in every room that may have people present?
   - □ No
   - □ Yes
10. Is the "duress" system or panic button able to generate a camera stream with computer pop-up messages so responding personnel can see a live view of the activation area?
    - □ No
    - □ Yes
11. Are hand-held 2-way radios/MARCS Radios used?
    - □ No
    - □ Yes

12. Are there intrusion alarms (door alarms, window bugs, glass break sensors) on the building?
    - □ No
    - □ Yes
13. Does the "duress" system or panic button work properly and is it tested and serviced on a regular basis?
    - □ No
    - □ Yes

SECURITY FORCE / DEPARTMENT

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #75, #79 and #84. Any additional items must be justified within the application.

1. Does the facility have a security manager or security department?
    - □ No
    - □ Yes
2. Is there security staff or law enforcement on duty during business hours? Nonbusiness hours?
    - □ No
    - □ Yes
3. Is there a security force?
    - □ No
    - □ Yes
4. Does the facility's security force have static posts?
    - □ No
    - □ Yes
5. Does the facility's security force have roving patrols?
    - □ No
    - □ Yes
6. Does the security force receive training?
    - □ No
    - □ Yes
7. Does the protective force have standard operating procedure manuals?
    - □ No
    - □ Yes
8. Does the protective force provide security escorts for visitors/employees?
    - □ No
    - □ Yes
9. Are security force personnel licensed or sworn?
    - □ No
    - □ Yes

10. Are yearly background checks conducted on licensed contract private security?
    - □ No
    - □ Yes
11. Do roving patrols report suspicious items and activity?
    - □ No
    - □ Yes

ACCESS CONTROL

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #3, #4, #14, #56, #58, #62, #63, #64, #65, #67, #76, #77, #78, #79, and #80. Any additional items must be justified within the application.

1. Is there controlled access into the building?
    - □ No
    - □ Yes
2. Are any exterior doors secured with electronic access control devices?
    - □ No
    - □ Yes
3. Is there a doorbell or other entry notification device located at the main entrance?
    - □ No
    - □ Yes
4. Is there a secure vestibule that separates the main entry from full building access?
    - □ No
    - □ Yes
5. Are access badges or FOBS issued?
    - □ No
    - □ Yes
6. Are multiple access levels in place based on need?
    - □ No
    - □ Yes
7. Does a system exist for removing terminated employees from a database?
    - □ No
    - □ Yes
8. Is the access control database regularly reviewed for accuracy?
    - □ No
    - □ Yes
9. Are access activity reports reviewed regularly?
    - □ No
    - □ Yes

10. Are after-hours access to the facility limited/monitored?
    - □ No
    - □ Yes

11. Do room doors have a door lock or door barricade device that can be locked?
    - □ No
    - □ Yes

12. Is there a backup power supply source for the access control systems?
    - □ No
    - □ Yes

SECURITY CONTROL ROOM

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #8, #9, #10, #11, #12, #13, #26, #63, #64, #65, #66, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is there a designated security control room and console in place to monitor security, fire alarm, and other building systems?
    - □ No
    - □ Yes
2. Is the location of the security room in a secure area with controlled and restricted access?
    - □ No
    - □ Yes
3. Is the security control room staffed continuously?
    - □ No
    - □ Yes
4. Are the security control room's access doors continuously locked to prevent unauthorized entry?
    - □ No
    - □ Yes

VIDEO SURVEILLANCE

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #1, #8, #9, #10, #11, #12, #13, #66, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is there a video surveillance system in use?
    - □ No
    - □ Yes
2. Is the system expandable?
    - □ No
    - □ Yes

3. Are camera images recorded?
   - □ No
   - □ Yes
4. Can the video system's storage capacity hold 30 days of video?
   - □ No
   - □ Yes
5. Are the cameras actively monitored?
   - □ No
   - □ Yes
6. Is the surveillance system networked and capable of remote monitoring by authorized personnel and first responders?
   - □ No
   - □ Yes
7. Can the system export historical video for forensic review?
   - □ No
   - □ Yes
8. Are the critical components of the system (recording devices, power supplies, etc.) in a secured location?
   - □ No
   - □ Yes
9. Have staff members been adequately trained on using the system?
   - □ No
   - □ Yes
10. Is there video coverage for all exterior doors?
    - □ No
    - □ Yes
11. Is there video coverage of the full building exterior?
    - □ No
    - □ Yes
12. Are security cameras in the vestibule?
    - □ No
    - □ Yes
13. Is there video coverage for all common areas?
    - □ No
    - □ Yes
14. Is there video coverage of restroom entries and stairwells?
    - □ No
    - □ Yes

15. Is there video coverage of all halls and cross halls?
    - □ No
    - □ Yes
16. Is there video coverage of high liability risk areas?
    - □ No
    - □ Yes
17. Is the facility's camera system regularly inspected and maintained?
    - □ No
    - □ Yes
18. Do the cameras have pan/tilt/zoom or panoramic capabilities?
    - □ No
    - □ Yes
19. Is there emergency backup power for cameras?
    - □ No
    - □ Yes

PERIMETER

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #3, #58, #60, #66, #67, #76, #77, #78 and #80. Any additional items must be justified within the application.

1. Is the property line free of debris?
    - □ No
    - □ Yes
2. Is the landscaping trimmed to allow direct line of sight in and out of the building?
    - □ No
    - □ Yes
3. Is there a perimeter fence or other type of barrier in place around the entire site?
    - □ No
    - □ Yes
4. Are there weak areas or breaches in the fence or barrier?
    - □ No
    - □ Yes
5. Are there openings in the fence or barrier controlled by gates?
    - □ No
    - □ Yes
6. Are the gates locked?
    - □ No
    - □ Yes

7. Are there bollards or other barriers protecting the building face from vehicular intrusion?
   - □ No
   - □ Yes

FACILITY LIGHTING

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #60, #76, #77 and #78. Any additional items must be justified within the application.

1. Is the lighting adequate, from a security perspective, for roadway access and parking areas?
   - □ No
   - □ Yes
2. Are pathways around the site illuminated to assist with movement and safety?
   - □ No
   - □ Yes
3. Is there adequate lighting around the exterior of the facility?
   - □ No
   - □ Yes
4. Is there adequate lighting at exterior doors?
   - □ No
   - □ Yes

PARKING / PARKING LOTS

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #26, #45, #64, #67, #68, #76, #77, #78, #79, #80 and #84. Any additional items must be justified within the application.

1. Is the parking lot patrolled?
   - □ No
   - □ Yes
2. Are radios or other communication devices available for use by those on patrol?
   - □ No
   - □ Yes
3. Are vehicles that frequent the facility (employees, volunteers, etc.) identified by decals, hang tags?
   - □ No
   - □ Yes
4. Are vehicles parked at the building screened, monitored, and/or inspected?
   - □ No
   - □ Yes

5. Does the facility have a policy to address vehicles parked for an extended period or suspicious vehicles (e.g., reporting to security, local law enforcement, and tow company)?
   - □ No
   - □ Yes
6. Are high-speed avenues of approach restricted?
   - □ No
   - □ Yes

BUILDING ENVELOPE (DOORS, WINDOWS, ROOF)

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #55, #56, #58, #62, #65, #67, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Do all exterior doors have working locks?
   - □ No
   - □ Yes
2. Are all exterior doors locked during business hours?
   - □ No
   - □ Yes
3. Are all exterior doors identified by signage or other markings?
   - □ No
   - □ Yes
4. Are all exterior windows numbered?
   - □ No
   - □ Yes
5. Are windows in exterior doors and sidelights outfitted with safety film?
   - □ No
   - □ Yes
6. Does the location of the main entrance allow for staff or volunteers to visually monitor its use?
   - □ No
   - □ Yes
7. Is the main entrance pathway in direct line of sight of staff or volunteers?
   - □ No
   - □ Yes
8. Do room doors have a window so administration can see in, if applicable (schools, child care, etc.?)
   - □ No
   - □ Yes
9. Are openings or portals on the roof secured to deny entry?
   - □ No
   - □ Yes

VISITOR CONTROL

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #3, #4, #5, #6, #7, #14, #63, #68, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is a (paper and pen) sign-in system in place that collects the name, address and reason for visiting and is monitored by staff and/or volunteers?
   - □ No
   - □ Yes
2. Do all visitors present a proof of identification?
   - □ No
   - □ Yes
3. Are all visitors handled in a consistent manner?
   - □ No
   - □ Yes
4. Are visitors issued a self-adhesive visitor pass, uniquely designed for the facility with a highly visible (from 3’-4’ away) “DATE VALID?”
   - □ No
   - □ Yes
5. Is a computer-based sign-in system in place that collects the name, address and reason for visiting and is monitored by staff and/or volunteers?
   - □ No
   - □ Yes
6. Does the sign-in system check visitors’ names against the National Sex Offenders Registry?
   - □ No
   - □ Yes
7. Are visitors required to be escorted at all times?
   - □ No
   - □ Yes
8. Are visitors/customers prevented from accessing unauthorized areas?
   - □ No
   - □ Yes
9. Does staff challenge or offer to assist people not wearing a visitor's pass or identification credentials?
   - □ No
   - □ Yes
10. Are all visitors required to sign out after their visit is complete?
    - □ No
    - □ Yes
11. Are visitor passes collected from visitors when they leave the building?
    - □ No
    - □ Yes

12. Do contractors working the facility have restricted access?
    - □ No
    - □ Yes

TECHNOLOGY

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #16, #17, #18, #19, #20, #21, #22, #23, #24, #25, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is up-to-date anti-virus software loaded on all devices that connect to the server?
    - □ No
    - □ Yes
2. Are individual firewalls loaded on all devices that connect to the server?
    - □ No
    - □ Yes
3. Is a network firewall in place?
    - □ No
    - □ Yes
4. Has staff been trained on the proper use of cyber security and equipment?
    - □ No
    - □ Yes
5. Is an uninterrupted power supply (UPS) unit connected to crucial network equipment?
    - □ No
    - □ Yes
6. Is encryption software used for sending/receiving sensitive materials?
    - □ No
    - □ Yes

KEY CONTROL PROCEDURES

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #62, #77, #78, #79 and #82. Any additional items must be justified within the application.

1. Is there a key control/management system? (i.e., inventory, securing spare keys)
    - □ No
    - □ Yes
2. Are all locks in good working order?
    - □ No
    - □ Yes

3. Are key audits conducted regularly?
   - □ No
   - □ Yes
4. Are master keys restricted to certain personnel?
   - □ No
   - □ Yes
5. Is there a system in place for retrieving keys from terminated employees and contractors?
   - □ No
   - □ Yes

OTHER

Please refer to the Authorized Equipment List for a detailed description of all available options to purchase for this section. Those specific to this section include item: #37, #44, #54, #67, #76, #77, #78 and #79. Any additional items must be justified within the application.

1. Is backup power connected to the security system in the event of a power failure?
   - □ No
   - □ Yes (Other - Generator)
2. Are background checks made on all new employees, volunteers and vendors?
   - □ No
   - □ Yes (Other – Fingerprint processing)
3. Does the facility have temporary barricading equipment?
   - □ No
   - □ Yes (Other – Barricade System)
4. If there are waste containers located around the building exterior, are they blast-resistant?
   - □ No
   - □ Yes

After a review of this assessment, what recommendations were made to improve safety and security at this facility? (Please describe the recommendations below)

Signature of the individual completing the assessment: ___________________________________