Maine Emergency Management Agency Homeland Security Division
Federal Fiscal Year 2024
US DHS/FEMA Nonprofit Security Grant Program Notice of Funding Opportunity - Sub-applicant
April 18, 2024

The following is a brief overview of the FY2024 NSGP and specific guidance needed for entities applying for funds. The Sub-applicant is responsible for ensuring that the proposed project fully complies with both Federal and MEMA guidance for the NSGP. Links to the federal guidelines for this program and other pertinent documents are provided within this document. The point of contact email for this grant is HSGrants.Maine@maine.gov. To review the full FEMA version of the NSGP NOFO, https://www.fema.gov/grants/preparedness/nonprofit-security/fy-24-nofo

The objective of the Nonprofit Security Grant Program is to provide funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist or other extremist attack. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts.

In FY 2024, FEMA identified one priority area related to some of the most serious threats that Sub-applicants should address with their NSGP funds: enhancing the protection of soft targets/crowded places. Focusing on forging partnerships to strengthen information sharing and collaboration and, although there are no requirements for information sharing between nonprofit organizations and federal, state, local, tribal, and territorial law enforcement, the NSGP seeks to bring nonprofit organizations into broader state and local preparedness efforts by removing barriers to communication and being more inclusive. See Appendix A for more information on funding priorities.

Eligible Applicants and Subrecipients

The State is the only eligible applicant for the grant applying to FEMA directly, the purpose of this "Sub-applicant NOFO" is for all applicants applying to the State and are considered subrecipients for the Nonprofit Security Program.

Nonprofit eligible applicants are:

1. Described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code. This includes entities designated as "private" (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501c3 entities. The organization cannot be a for-profit/fundraising extension of a nonprofit organization. While these for-profit or fundraising extensions may be associated with the eligible nonprofit organization, NSGP funding cannot be used to benefit those extensions and therefore they will be considered ineligible applications. If the funding being sought is for the benefit of a for-profit/fundraising extension, then that would constitute an ineligible subaward since only nonprofit organizations are eligible subrecipients.

2. Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attack.

3. Nonprofit sub-applicants with one site/location/physical address may apply for up to $150,000 for that site/location/physical address. Nonprofit sub-applicants with multiple site/location/physical address may apply for up to $150,000 per site/location/physical address, for up to three site/location/physical addresses, for a maximum of $450,000 per nonprofit sub-applicant per state and funding source. If a nonprofit sub-applicant applies for multiple site/location/physical address, it must submit one complete IJ for each site/location/physical address. Each site/location/physical address will have a physical address and not a PO Box.

4. Nonprofit sub-applicants are required to self-identify with one of the following four categories in the IJ as part of the application process:

    a. Ideology-based/Spiritual/Religious
    b. Educational
    c. Medical
    d. Other

Note: The Internal Revenue Service (IRS) does not require certain organizations such as churches, mosques, and synagogues to apply for and receive a recognition of exemption under section 501(c)(3) of the IRC. Such organizations are automatically exempt if they meet the requirements of section 501(c)(3). These organizations are not required to provide recognition of exemption. For organizations that the IRS requires to apply for and receive a recognition of exemption under section 501(c)(3), the State will require recognition of exemption.

All entities wishing to do business with the federal government must have an active Unique Entity Identifier (UEI). To review the steps in this process, click here. Nonprofit organization sub-applicants applying for NSGP funding through the SAA must have a UEI ***at the time they receive a subaward***. Nonprofit organizations must register in SAM.gov to obtain the UEI but are not required to have an active registration in SAM at the time of application. Further guidance on obtaining a UEI in SAM.gov can be found on the SAM.gov website. Nonprofit sub-applicants are also reminded that if they have previously applied for another federal grant, they should use the same UEI and EIN from those prior applications to save time.

National Incident Management System (NIMS) Implementation
Recipients receiving NSGP funding are strongly encouraged to implement NIMS. NIMS guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System.

Incident management activities require carefully managed resources (personnel, teams, facilities, equipment, and supplies). NIMS defines a national, interoperable approach for sharing resources, coordinating, and managing incidents, and communicating information. Incident management refers to how incidents are managed across all homeland security activities, including prevention, protection, mitigation, response, and recovery.

Utilization of the standardized resource management concepts such as typing, credentialing, and inventorying promote a strong national mutual aid capability needed to support delivery of core capabilities. Recipients should manage resources purchased or supported with FEMA grant funding according to NIMS resource management guidance.

Key Dates

Sub-applicant NOFO Posted	04/19/2024
Sub-applicant Application Due Date	05/31/2024 (5PM)
FEMA Award Notification to MEMA	September 2024 (expected)
MEMA Award Announcements	October 2024 (subject to change based on FEMA release)

Goals and Project Based Process
This is a project-based grant and project acceptance will be determined by identified criteria, therefore it will be imperative for applicants to clearly outline the need for their proposed project and identify the capability gap(s) that have been identified in their vulnerability assessment. For more information on the vulnerability assessment, see "Investment Justification and Projects" section.
***Note: All funding and awards are contingent upon MEMA's receipt of FY2024 NSGP funds from DHS/FEMA.**

Sub-application Submission to MEMA

- Projects must be prepared and submitted using the MEMA FY2024 NSGP Project Submission Portal.
- Projects submitted in other formats will not be reviewed or considered for funding.
- Active UEI number (required at the time of the ***award***)
- Vulnerability assessment will be uploaded but will not take the place of the Investment Justification (see Appendix B).
- If the organization is exempt from 501c3 status, please provide IRS documentation.
- State of Maine Vendor Code or application for Vendor Code, documents are posted on the MEMA website.

Investment Justification and Projects

Each investment justification will:

1. Have a description of/include:
    a. Be for the site/location/physical address that the nonprofit occupies at the time of application and will not exceed $150,000.00.
    b. **Address an identified risk, including threat and vulnerability, regardless of whether it is submitting for similar projects at multiple sites.**
    c. Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA.
    d. Be both feasible and effective at reducing the risks for which the project was designed.
    e. Be able to be fully completed within the three-year period of performance.
    f. Be consistent with all applicable requirements outlined in the funding notice and the FEMA Preparedness Grants Manual.
    g. Provide a description of the nonprofit organization to include symbolic value of the site as a highly recognized national or historical institution or as a significant institution within the community that renders the site as a possible target of terrorism and other extremist attacks.
    h. Provide a description of their nonprofit organization to include any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local preparedness efforts.
    i. Discuss specific threats or attacks against the nonprofit organization or closely related organization.
    j. Describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack.
    k. Address potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist or other extremist attack.
    l. Describe the proposed facility hardening activities, projects, and/or equipment and relate their proposals to the vulnerabilities described in the "Risk" Section.
    m. Describe the proposed facility hardening activity focus on the prevention of and/or protection against the risk of a terrorist or other extremist attack.
    n. Propose equipment, activities, and/or projects tied to a vulnerability.
    o. Include and describe the milestones and the associated key activities that lead to the milestone event over the NSGP period of performance.
    p. Justify the effectiveness of the proposed management team's roles and responsibilities and the governance structure to support the implementation of the Investment.
    q. Describe the outcomes/outputs that would indicate that the Investment will be successful.

2. Each nonprofit sub-applicant must include a vulnerability assessment **unique to the site** the IJ is being submitted.
3. Each nonprofit sub-applicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk. The State and FEMA will use the Mission Statement along with the nonprofit sub-applicant's self-identification in **t**he IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious; 2) Educational; 3) Medical; or 4) Other.

Funding Restrictions and Allowable Costs

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award, or the Preparedness Grants Manual. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance).

Federal funds made available through this award may be used for the purpose set forth in this NOFO, the FEMA Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award.

Award funds may not be used for matching funds for any other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the FEMA Preparedness Grants Manual for more information on funding restrictions and allowable costs.

Planning

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs as well as those with limited English proficiency. Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, using the Infrastructure Resilience Planning Framework and related CISA resources.

Examples of planning activities allowable under this program include:

- Development and enhancement of security plans and protocols.
- Development or further strengthening of security assessments.
- Emergency contingency plans.
- Evacuation/Shelter-in-place plans.
- Coordination and information sharing with fusion centers.
- Other project planning activities with prior approval from FEMA.

Equipment

Allowable costs are focused on facility hardening and physical security enhancements. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist or other extremist attack.

This equipment is limited to select items on the Authorized Equipment List (AEL):

- 03OE-03-MEGA System, Public Address, Handheld or Mobile
- 03OE-03-SIGN Signs, Restricted access and caution warning signs that preprinted or field printable
- 04AP-05-CRED System, Credentialing
- 04AP-09-ALRT Systems, Public Notification and Warning
- 04AP-11-SAAS Applications, Software as a Service
- 05AU-00-TOKN System, Remote Authentication
- 05EN-00-ECRP Software, Encryption
- 05HS-00-MALW Software, Malware/Anti-Virus Protection
- 05HS-00-PFWL System, Personal Firewall
- 05NP-00-FWAL Firewall, Network
- 05NP-00-IDPS System, Intrusion Detection/Prevention

- 06CP-01-PORT Radio, Portable
- 06CP-01-REPT, Repeater, Electronic devise that receives a weak or low-level signal and retransmits
- 06CC-02-PAGE Services/Systems, Paging
- 06CP-03-ICOM Intercom
- 06CP-03-PRAC Accessories, Portable Radio
- 10GE-00-GENR Generators
- 13IT-00-ALRT System, Alert/Notification
- 10PE-00-UPS Supply, Uninterruptible Power, Systems that compensate for power loss to serviced equipment
- 14CI-00-COOP System, Information Technology Contingency Operations
- 14EX-00-BCAN Receptacles, Trash, Blast-Resistant
- 14EX-00-BSIR Systems, Building, Blast/Shock/Impact Resistant
- 14SW-01-ALRM Systems/Sensors, Alarm
- 14SW-01-ASTN Network, Acoustic Sensor Triangulation, Network of deployed acoustic sensors for data integration and analysis.
- 14SW-01-DOOR Doors and Gates, Impact Resistant
- 14SW-01-LITE Lighting, Area, Fixed
- 14SW-01-PACS System, Physical Access Control
- 14SW-01-SIDP Systems
- 14SW-01-SIDV Systems, Vehicle Identification
- 14SW-01-SNSR Sensors/Alarms, System and Infrastructure Monitoring, Standalone
- 14SW-01-VIDA Systems, Video Assessment, Security
- 14SW-01-WALL Barriers: Fences; Jersey Walls
- 15SC-00-PPSS Systems, Personnel/Package Screening
- 21GN-00-INST Installation
- 21GN-00-TRNG Training and Awareness

Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment, whether with NSGP funding or other sources of funds.

In addition, subrecipients that are using NSGP funds to support emergency communications equipment activities must comply with the SAFECOM Guidance on Emergency Communications Grants, including provisions on technical standards that ensure and enhance interoperable communications. Any proposal that includes an Interoperable Communications component must align to the Statewide Communication Interoperability Plan (SCIP) and requires coordination, consultation, and approval from the Statewide Interoperability Coordinator (SWIC).

NOTE: Nonprofits should indicate in their budget narratives if a cost includes shipping and/or tax. It is not required to break the costs out as separate from the relevant purchase(s).

Applicants and sub-applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high-cost items, and those subject to rapid technical advances. Large equipment purchases must be identified and explained. The installation of certain equipment may trigger Environmental Planning and Historic Preservation (EHP) requirements.

Exercises

Funding may be used to conduct security-related exercises. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation.

Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low risk setting. All shortcomings or gaps—including those identified for children and individuals with access and functional needs—should be identified in an improvement plan. Improvement plans should be dynamic documents with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

Maintenance and Sustainment

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable under all active and future grant awards, unless otherwise noted.

Preparedness grant funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

Construction and Renovation

NSGP funding may **not** be used for construction and renovation projects without prior written approval from FEMA. In some cases, the installation of equipment may constitute construction and/or renovation. All subrecipients of NSGP funds must request and receive prior approval from FEMA before any NSGP funds are used for any construction or renovation.

Training

Nonprofit organizations may use NSGP funds for the following training-related costs:

- Employed or volunteer security staff to attend security-related training within the United States.
- Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., "train-the-trainer" type courses); and
- Nonprofit organization's employees, or members/congregants to receive on-site security training.

Allowable training-related costs under the NSGP are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and travel expenses are **not** allowable costs.

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, facility hardening, and terrorism/other extremism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist/other extremist threats, Active Shooter training, and emergency first aid training.

Additional examples of allowable training courses include: "Stop The Bleed" training, kits/equipment, and training aids; First Aid and other novice level "you are the help until help arrives" training, kits/equipment, and training aids; and Automatic External Defibrillator (AED) and AED/Basic Life Support training, kits/equipment, and training aids.

Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization's Investment Justification (IJ). Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Proposed attendance at training courses and all associated costs using the NSGP must be included in the nonprofit organization's IJ.

Contracted Security Personnel

Contracted security personnel are allowed under this program only as described in the NOFO and Manual and comply with guidance set forth in IB 421b and IB 441. NSGP funds may not be used to purchase equipment for contracted security.

The subrecipient must be able to sustain this capability in future years without NSGP funding, and a sustainment plan will be required as part of the closeout package for any award funding this capability.

Unallowable Costs

The following projects and costs are considered ineligible for award consideration:

- Organization costs, and operational overtime costs.
- Hiring of public safety personnel.
- General use expenditures.
- Overtime and backfill.
- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities.
- The development of risk/vulnerability assessment models.
- Initiatives that fund risk or vulnerability security assessments or the development of the IJ.
- Initiatives in which federal agencies are the beneficiary or that enhance federal property.
- Initiatives which study technology development.
- Proof-of-concept initiatives.
- Initiatives that duplicate capabilities being provided by the Federal Government.
- Organizational operating expenses.
- Reimbursement of pre-award security expenses.
- Cameras for license plate readers/license plate reader software.
- Cameras for facial recognition software.
- Weapons or weapons-related training; and
- Knox boxes.

Environmental Planning and Historic Preservation (EHP) Compliance

Most subawards are subject to EHP review. Subrecipients receiving in part or full grant funds must submit, through MEMA, an EHP review and approval before initiation, unless expressly exempted from the requirement. Projects that may trigger an environmental review include, but not limited to, debris removal, emergency protective measures, equipment installation, new construction, and ground disturbance. Exercise and Training projects with any field-based component (drill and full-scale exercises) require EHP review. Failure to comply with this requirement could result in project delays and denial of funding.

Subrecipients should allot at least 45-60 days for the EHP approval process.

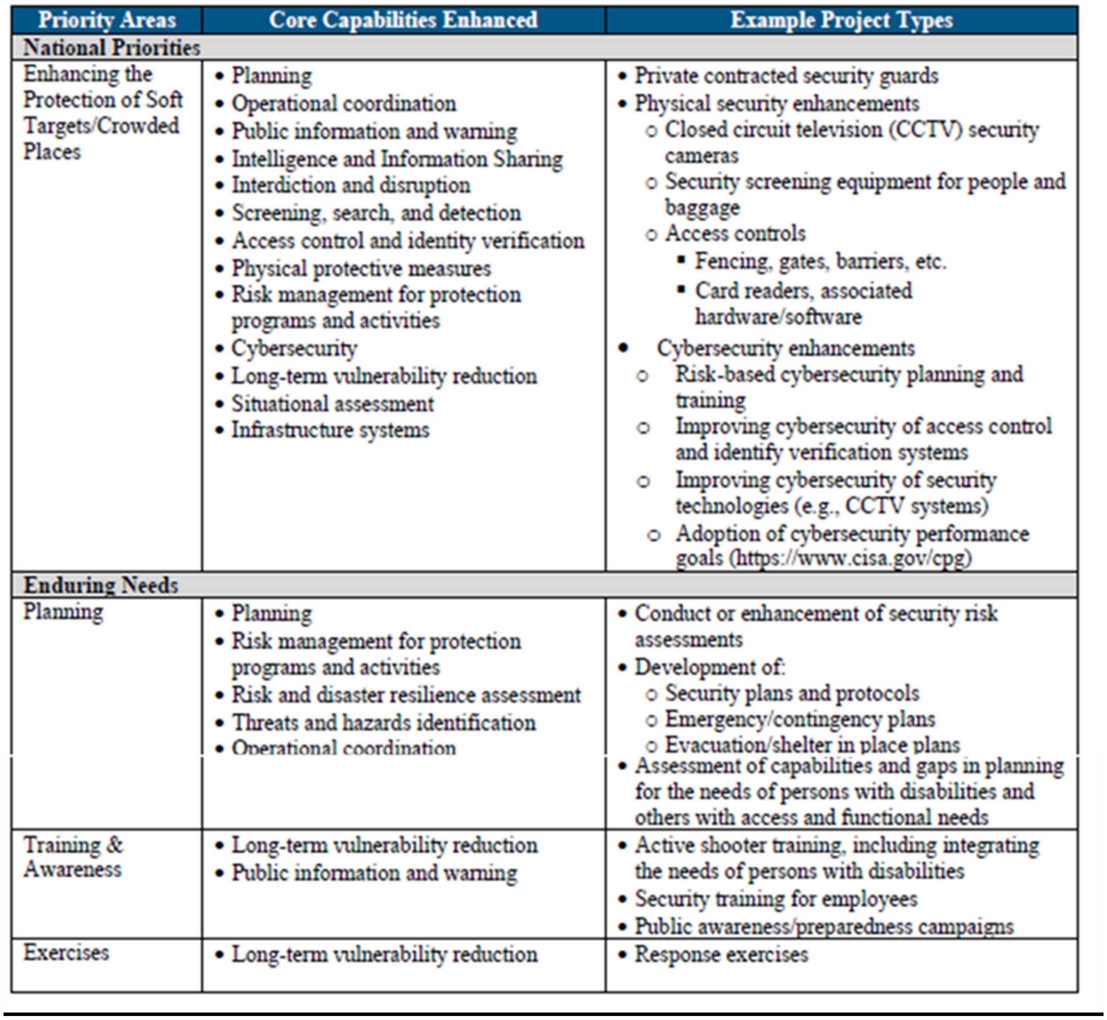
Reporting

Subrecipients are required to submit progress reports each calendar quarter. MEMA will provide the subrecipient with a project tracker and tools to complete these reports.

Monitoring and Oversight

MEMA or FEMA have the right, at all reasonable times, to make site visits or conduct desk reviews to review project accomplishments and management control systems to review award progress and to provide any required technical assistance. During site visits or desk reviews, MEMA/FEMA will review recipients' files related to the award. As part of any monitoring and program evaluation activities, recipients must permit MEMA/FEMA, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to MEMA/FEMA requests for information relating to the award.

Appendix A: FEMA Funding Priorities



Priority Areas	Core Capabilities Enhanced	Example Project Types
National Priorities		
Enhancing the Protection of Soft Targets/Crowded Places	• Planning • Operational coordination • Public information and warning • Intelligence and Information Sharing • Interdiction and disruption • Screening, search, and detection • Access control and identity verification • Physical protective measures • Risk management for protection programs and activities • Cybersecurity • Long-term vulnerability reduction • Situational assessment • Infrastructure systems	• Private contracted security guards • Physical security enhancements ○ Closed circuit television (CCTV) security cameras ○ Security screening equipment for people and baggage ○ Access controls ▪ Fencing, gates, barriers, etc. ▪ Card readers, associated hardware/software • Cybersecurity enhancements ○ Risk-based cybersecurity planning and training ○ Improving cybersecurity of access control and identify verification systems ○ Improving cybersecurity of security technologies (e.g., CCTV systems) ○ Adoption of cybersecurity performance goals (https://www.cisa.gov/cpg)
Enduring Needs		
Planning	• Planning • Risk management for protection programs and activities • Risk and disaster resilience assessment • Threats and hazards identification • Operational coordination	• Conduct or enhancement of security risk assessments • Development of: ○ Security plans and protocols ○ Emergency/contingency plans ○ Evacuation/shelter in place plans • Assessment of capabilities and gaps in planning for the needs of persons with disabilities and others with access and functional needs
Training & Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training, including integrating the needs of persons with disabilities • Security training for employees • Public awareness/preparedness campaigns
Exercises	• Long-term vulnerability reduction	• Response exercises

Appendix B: Vulnerability/Risk Assessment & CISA Resources

CISA: Protecting Houses of Worship Assessment Resources:

- https://www.cisa.gov/faith-based-organizations-houses-worship
- https://www.cisa.gov/resources-tools/resources/paper-based-houses-worship-security-self-assessment-and-user-guide

CISA: Security Assessment at First Entry (SAFE)

- https://www.cisa.gov/resources-tools/services/security-assessment-first-entry