FAITH BASED RESOURCES

Baltimore-Washington Conference
The United Methodist Church

Faith Based Community Resource Page

- Goal of page is empowering the user to build a facility security program
  - Describes a simple process to work through a risk reduction process
  - Brief explanation of how to use the available resources
  - Focus areas for the "process"
  - Contains the building blocks for a facility or community risk reduction program
  - Continually updated to reflect new resources or guidance

  https://www.cisa.gov/faith-based-organizations-houses-worship

Using Faith-Based Four-Step Process…

STEP 1
Start the Process

STEP 2
Conduct Assessment

STEP 3
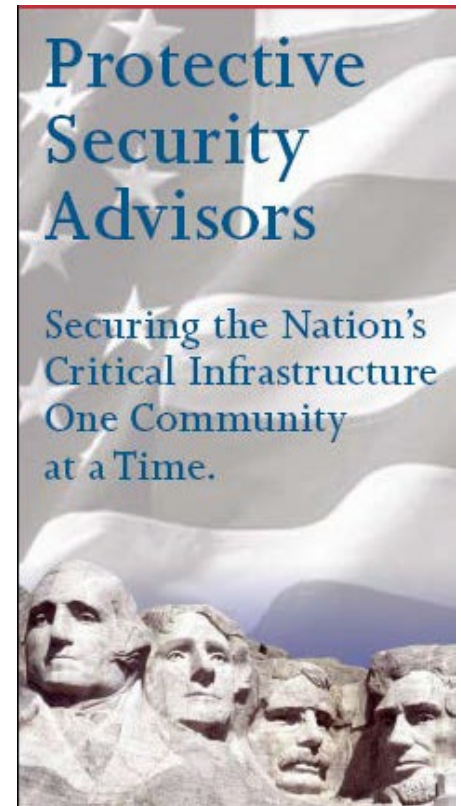Implement Security Improvements

STEP 4
Test Your Improvements

Step 1…

STEP 1
Start
the Process

STEP 2
Conduct
Assessment

STEP 3
Implement Security
Improvements

STEP 4
Test Your
Improvements

DHS / CISA & Local First Responders

Assistance with:

- **Connecting you with your state & local partners**
  - Resources
  - Threat information

- **Assessing vulnerabilities**

- **Exercises**

- **Training**
  - Run Hide Fight
  - Recognizing suspicious activity
  - Bombing Prevention

Protective Security Advisors

Securing the Nation's Critical Infrastructure One Community at a Time.

Houses of Worship Security Guide

Goals

Conduct original research to analyze incidents of targeted violence against houses of worship between 2009 and 2019

Develop a security framework that can be tailored to houses of worship of all sizes and denominations

Audience

Houses of worship and faith-based organizations looking to improve security

Available now:

cisa.gov/faith-based-organizations-houses-worship

MITIGATING ATTACKS ON HOUSES OF WORSHIP

Security Guide

DECEMBER 2020

U.S. Department of Homeland Security
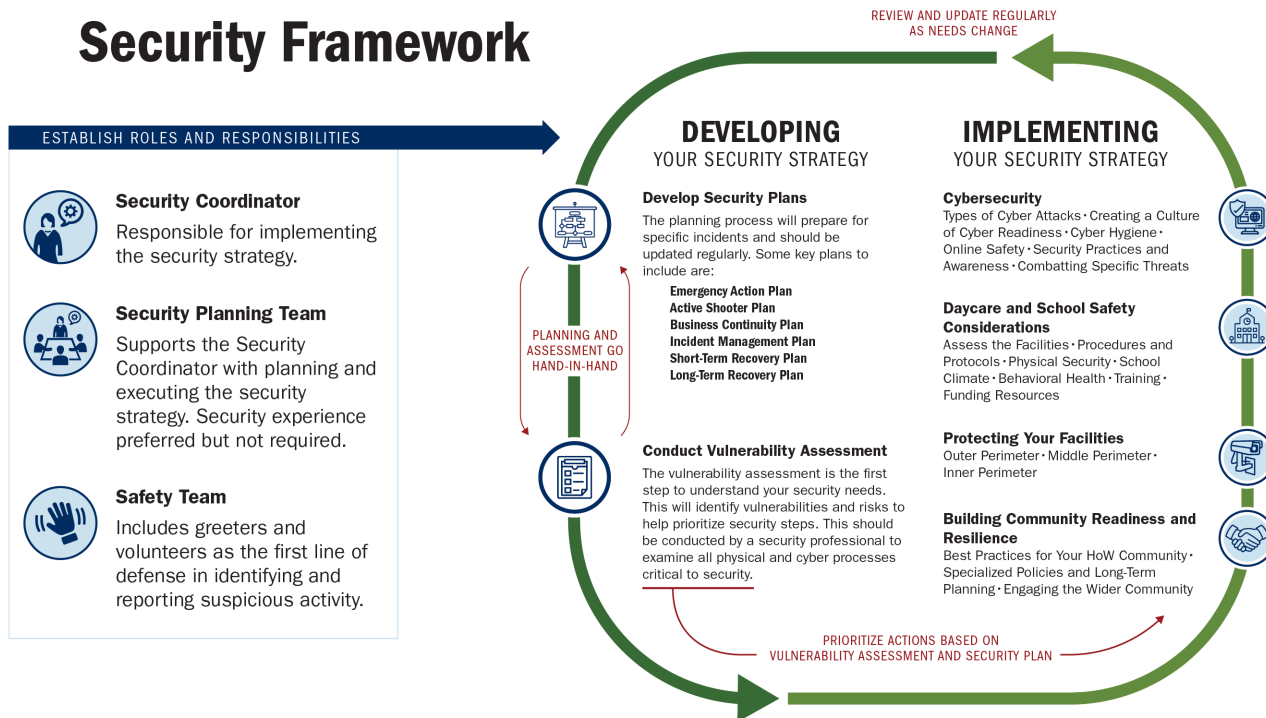Cybersecurity and Infrastructure Security Agency
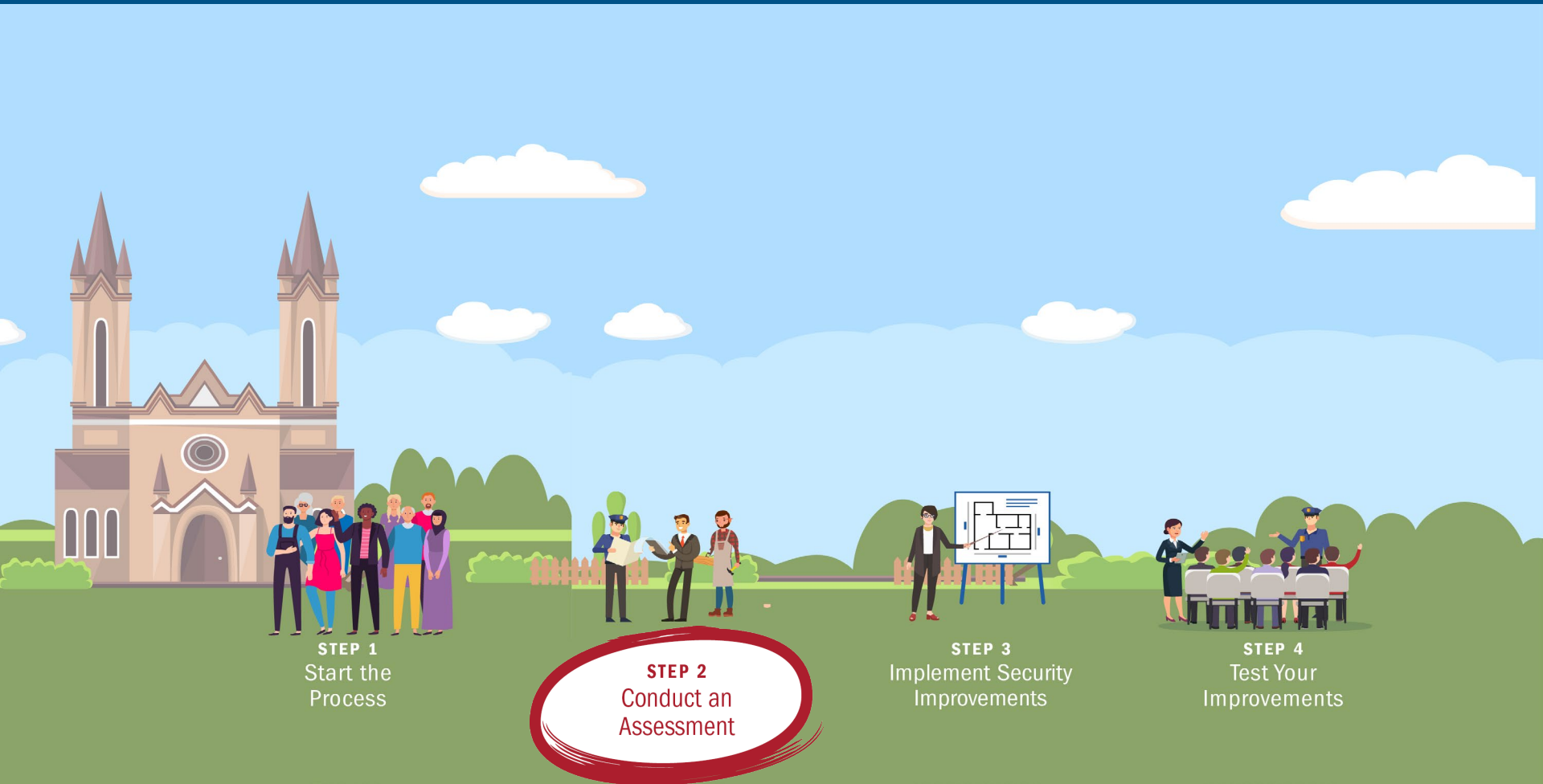
Guide developed in coordination with:

· Federal, state, local, tribal, and territorial partners
· Faith-based organizations
· Subject matter experts in security for houses of worship

Houses of Worship Security Guide Recommendations

Security Framework

ESTABLISH ROLES AND RESPONSIBILITIES

Security Coordinator
Responsible for implementing the security strategy.

Security Planning Team
Supports the Security Coordinator with planning and executing the security strategy. Security experience preferred but not required.

Safety Team
Includes greeters and volunteers as the first line of defense in identifying and reporting suspicious activity.

REVIEW AND UPDATE REGULARLY AS NEEDS CHANGE

DEVELOPING
YOUR SECURITY STRATEGY

Develop Security Plans
The planning process will prepare for specific incidents and should be updated regularly. Some key plans to include are:

Emergency Action Plan
Active Shooter Plan
Business Continuity Plan
Incident Management Plan
Short-Term Recovery Plan
Long-Term Recovery Plan

PLANNING AND ASSESSMENT GO HAND-IN-HAND

Conduct Vulnerability Assessment
The vulnerability assessment is the first step to understand your security needs. This will identify vulnerabilities and risks to help prioritize security steps. This should be conducted by a security professional to examine all physical and cyber processes critical to security.

IMPLEMENTING
YOUR SECURITY STRATEGY

Cybersecurity
Types of Cyber Attacks · Creating a Culture of Cyber Readiness · Cyber Hygiene · Online Safety · Security Practices and Awareness · Combatting Specific Threats

Daycare and School Safety Considerations
Assess the Facilities · Procedures and Protocols · Physical Security · School Climate · Behavioral Health · Training · Funding Resources

Protecting Your Facilities
Outer Perimeter · Middle Perimeter · Inner Perimeter

Building Community Readiness and Resilience
Best Practices for Your HoW Community · Specialized Policies and Long-Term Planning · Engaging the Wider Community

PRIORITIZE ACTIONS BASED ON VULNERABILITY ASSESSMENT AND SECURITY PLAN

Step 2…

STEP 1
Start the Process

STEP 2
Conduct an Assessment

STEP 3
Implement Security Improvements

STEP 4
Test Your Improvements

CISA SAFE Tool

- In-person assessment of your facility with a custom written report …

- The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats.

- The SAFE tool is suited for all facilities, including houses of worship

FBO-HOW Security Self-Assessment

FBO-HOW Security Self-Assessment

The assessment, when completed, will provide an easy to follow road map for implementing suggested voluntary options for consideration. These options are based on current best practices designed to improve facility security and preparedness:

The focus areas of the assessment include the following.

Security and Safety/Emergency Management	Perimeter Security/ Delineation	Parking and Barriers	Access Control/ Entry Control	Closed-circuit Video (CCV)/ Video Surveillance Systems (VSS)

FBO-HOW Security Self-Assessment

- Easy to use

- Designed for the minimally experienced assessor

- Outputs include:
  - ✓ Executive report for use in justifications (Word)
  - ✓ Action Item lists (Word & Excel)
  - ✓ Options for consideration
  - ✓ References

Houses Of Worship

Save Data Clear all Data

Introduction

Assessment Details

Security / Emergency Management

Security Force

Perimeter Security / Delineation

Parking and Barriers

Access Control / Easy Control

Closed-circuit Video / Video Surveillance Systems

Action Items
View / Export as csv file

Create Report
View / Print Formatted Report

Questions Only
View / Print Complete list of Questions Only

References

Houses Of Worship Security Self-Assessment Details

When filling out this self-assessment, consider significant areas and assets at the house of worship. Significant areas and assets may be critical components that support the facility's mission or unique elements of the facility. They may represent key vulnerabilities or areas of interest to an attacker. Potential significant areas and assets at a house of worship include the following:

- Sanctuary or Primary Gathering Area: The most sacred part of a house of worship, where congregants gather for worship services, prayer, recitations, and other religious activities. Generally, the most populated area during meeting times, thus often an area for attack by an active shooter.
- Fellowship Hall: Where congregants gather for meals, workshops, and other communal activities. May include a kitchen and eating areas or serve as a gymnasium.
- Financial Office: Where donations are stored during and after meetings. May be targeted for theft.
- Religious Exhibit, Display, Artifact, or Symbol: May be a permanent feature of the facility or temporarily erected for holidays or special events. May be a target for vandalism or theft.
- Facility Vehicles: Usually vans or buses belonging to the house of worship. May be used to transport congregants and visitors to and from the facility as well as offsite activities.

Please Contact CISA at Central@CISA.GOV✉ if you have any questions while performing a Houses of Worship Security Self-Assessment

To begin, enter the Facility Name and Date below to start a new self-assessment, or load a previously saved Houses of Worship Security Self-Assessment file to continue working on it. Then click the "Continue with Houses of Worship Security Self-Assessment" button.

Browse to saved data file

Choose File   No file chosen

Then click button   Load selected saved data

FBO-HOW Security Self-Assessment

THE SELF-ASSESSMENT IN ACTION

Question	Very Low	Low	Medium	High	Very High
1. Does the house of worship have a security manager or security committee to make security management decisions?	The house of worship does not have a security manager or committee.	The house of worship has a security manager or committee, but security management activities are sporadic. **Your self-identified level of security**	The house of worship has a security manager or committee. Security management activities are regularly scheduled, but not coordinated with other committees, departments, or groups (e.g., special events planning, childcare).	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, but additional personnel are needed to support the facility's security mission.	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, and staffing levels fully support the facility's security mission.
Option for Consideration	**Very Low**	**Low**	**Medium**	**High**	**Very High**
	Designate an individual as a security manager or a group of individuals as a security committee, and ensure that person or group is responsible for developing, implementing, and coordinating all security-related activities. If the manager or committee members have no security or law enforcement background, make sure they reach out to local law enforcement to become acquainted. Provide security management training and/or access to training materials and resources.	Schedule regular meetings to review security procedures and incidents. **Your starting point for improving security**	Coordinate safety and security planning with other committees, departments, and groups. Continual Improvement Approach	Hire or appoint additional personnel to support the facility's security mission.	Regularly assess the facility's security management program. Conduct security surveys, risk assessments, and threat assessments of the facility and neighboring areas. Implement best practices based on collaborative relationships and new or updated resources.

- **Background:** Security or safety managers (or volunteer security or safety personnel) are responsible for the effective implementation of security/safety policies, programs, directives, and training within their house of worship. Security or safety committees (also known as volunteer security teams or volunteer safety teams or departments) are a group of people working together to fulfill this same purpose. They may include religious leaders, congregants, security professionals, and first responders.
- **References:** (1) ASIS Houses of Worship Committee, *Recommended Best Practices for Securing Houses of Worship Around the World*, 2017, accessed January 13, 2020, asisonline.org/globalassets/get-involved/councils/documents/best-practices-securing-houses-of-worship.pdf (2) Interagency Security Committee (ISC), *Facility Security Plan: An Interagency Security Committee Guide,* 1st edition, 2015, accessed January 13, 2020, cisa.gov/publication/isc-facility-security-plan-guide.
- **For more information:**
  - Cybersecurity and Infrastructure Agency (CISA), "Hometown Security," 2020, accessed April 29, 2020, cisa.gov/hometown-security.
- State of New Jersey Office of Homeland Security and Preparedness, *Role of Security Coordinators*, undated, accessed January 14, 2020, static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/5a4d52ee53450af96083504f/1515016942789/Role+of+Security+Coordinators.pdf.

DHS Protective Security Advisors
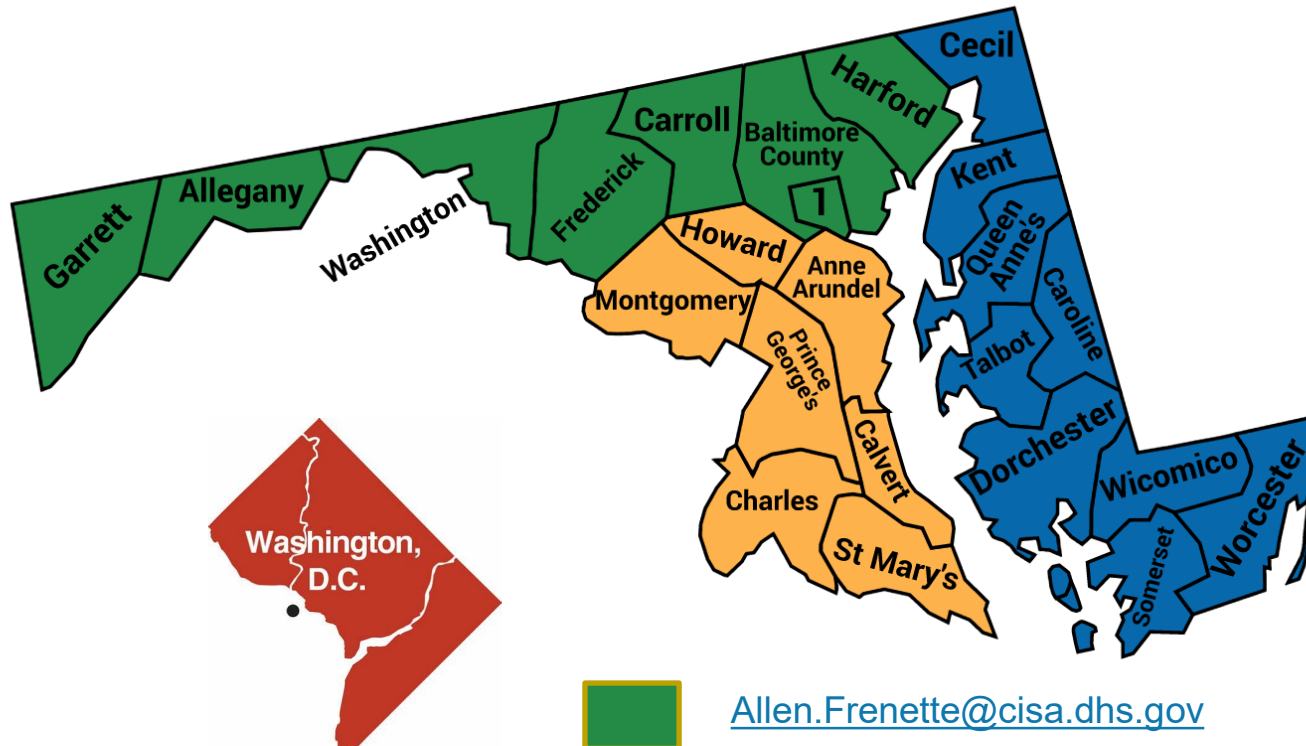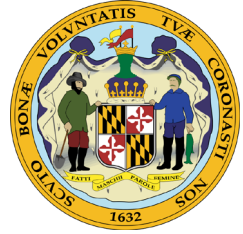
Allen.Frenette@cisa.dhs.gov

David.Johnston@cisa.dhs.gov

Ken.Greeson@hq.dhs.gov

Daniel.Genua@cisa.dhs.gov

February 22, 2022

Step 3…

STEP 1
Start the Process

STEP 2
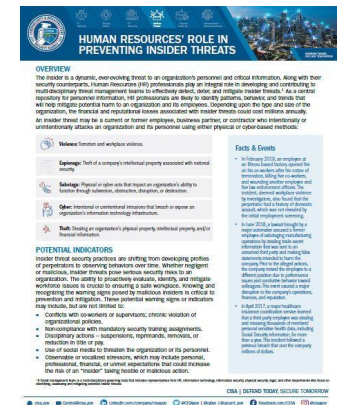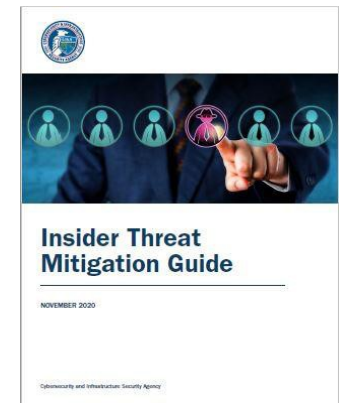Conduct Assessment

STEP 3
Implement Security Improvements

STEP 4
Test Your Improvements

CISA Resources

- Insider Threat Mitigation

- Active Assailant & Medical Training

- De-Escalation Training

Best Practice

John Wesley United Methodist Church

IP Video Door Intercom
and
Fob Access Reader

(Right side of main entrance)

John Wesley United Methodist Church

Day/Night Indoor/Outdoor
High-Resolution Camera

(Right side of main entrance)

John Wesley United Methodist Church

Camera in Narthex

(Adjacent to sanctuary entrance)

John Wesley United Methodist Church

Main Monitor & Answer Station

(Church conference room)

John Wesley United Methodist Church
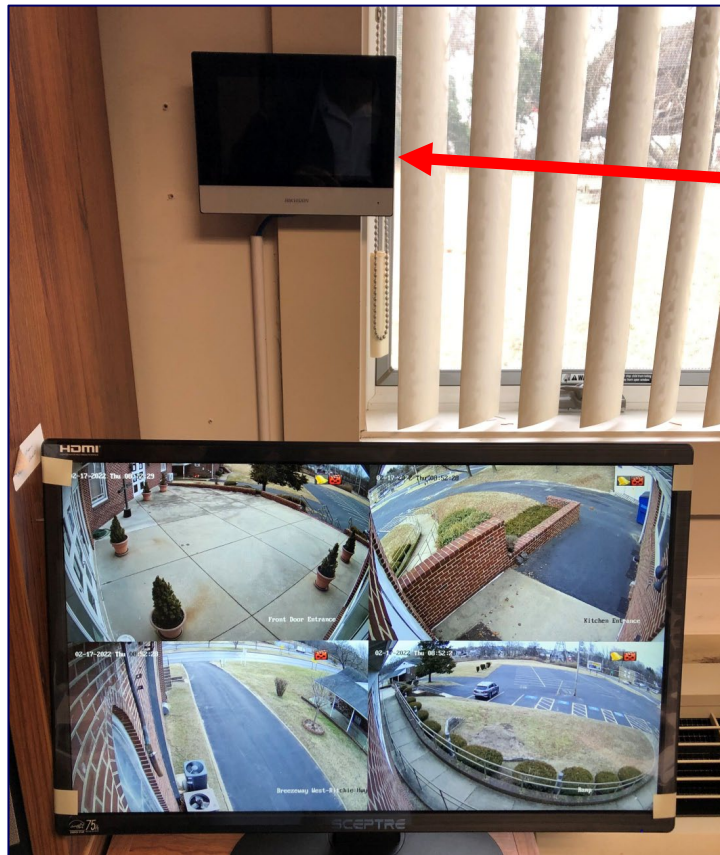
Monitor & Answer Station

(Secretary's office)

John Wesley United Methodist Church

Digital Quality Ethernet (Cat 5/6+) Cabling

(Custom installed throughout the Church)

Step 4…

STEP 1
Start the
Process

STEP 2
Conduct
Assessment

STEP 3
Implement Security
Improvements

STEP 4
Test your
Improvements

DHS Protective Security Advisors
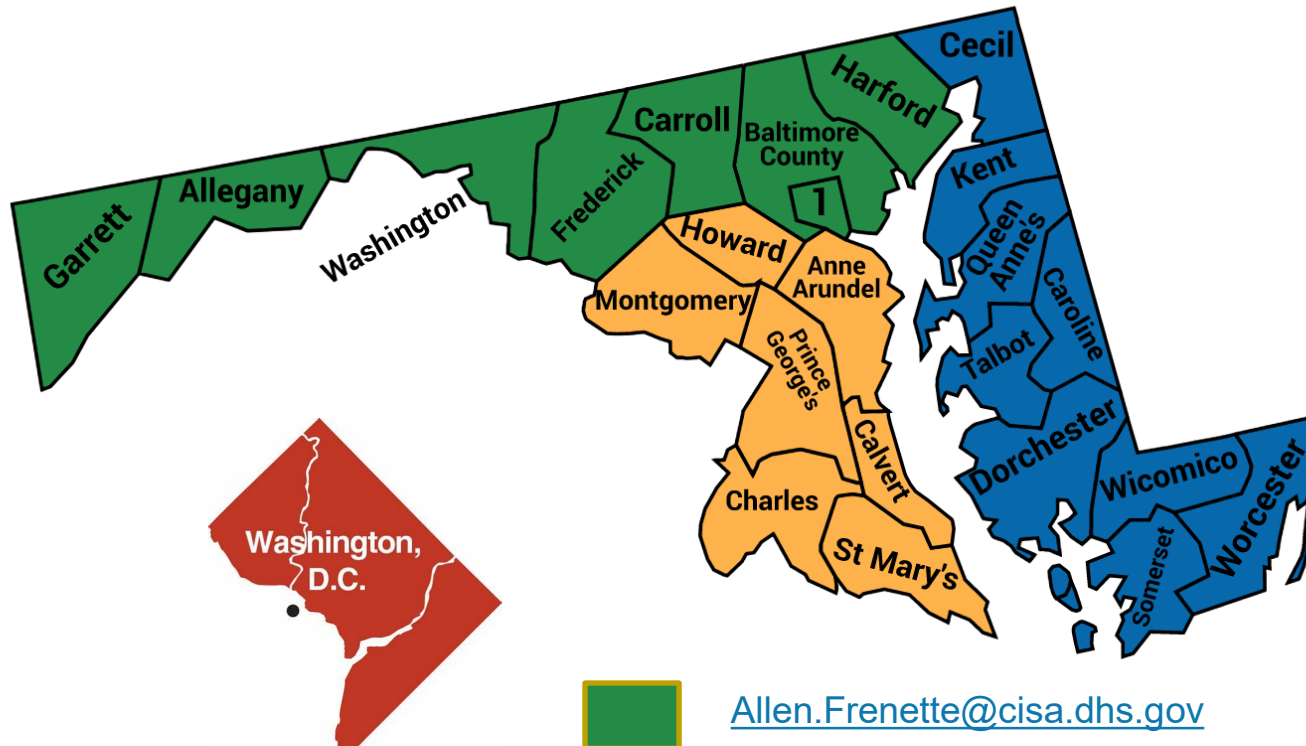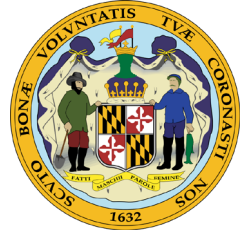
Allen.Frenette@cisa.dhs.gov

David.Johnston@cisa.dhs.gov

Ken.Greeson@hq.dhs.gov

Daniel.Genua@cisa.dhs.gov

February 22, 2022

Faith Based Community Resource Page

- Goal of page is empowering the user to build a facility security program
  - Describes a simple process to work through a risk reduction process
  - Brief explanation of how to use the available resources
  - Focus areas for the "process"
  - Contains the building blocks for a facility or community risk reduction program
  - Continually updated to reflect new resources or guidance

  https://www.cisa.gov/faith-based-organizations-houses-worship

What is NSGP and who is eligible?

- Authorized by Congress and implemented by DHS to help strengthen the nation's communities against potential terrorist attacks. NSGP supports the goal to Strengthen National Preparedness and Resilience.
- A **competitive** grant program intended to provide federal funding for physical enhancement and other security-related activities to nonprofit organizations that are at risk of a terrorist attack.
- *Applicants must be 501(c)(3) nonprofit organizations to be eligible.*

What Expenditures are eligible under NSGP ?

Specific investments generally fall into one of the following eight allowable expense categories:

1. Construction
2. Equipment
3. Exercises
4. Management & Administration (M&A)
5. Organization
6. Operational Activities
7. Planning
8. Training/Security

NSGP Timeline

- February/ March - Notice of Funding Opportunity (NOFO) NSGP
- March/ April - Pre-application Webinar hosted by MDEM
- April - Applications due to SAA
    - UASI Region vs. NCR Region vs State applications
    - Applications will be scored based on Scoring Tool
- May - Applications due to DHS/ FEMA
- September 1 - start date (30 month awards)

Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

NSGP Requirements

- Investment Justification
- Mission Statement
- Vulnerability Assessment

The mission of the Maryland Department of Emergency Management is to proactively reduce disaster risks and reliably manage consequences through collaborative work with Maryland's communities and partners.

Lola Parker

Lola.Parker2@maryland.gov

(443) 381-3290