KAUA'I HISTORIC PRESERVATION REVIEW COMMISSION

GERALD IDA, CHAIR
SUSAN REMOALDO, VICE CHAIR

LEE GATELY, MEMBER
KATHLEEN KIKUCHI-SAMONTE, MEMBER
CAROLYN LARSON, MEMBER
STEPHEN LONG, MEMBER
SANDI QUINSAAT, MEMBER
AUBREY SUMMERS, MEMBER
VICTORIA WICHMAN, MEMBER

RECEIVED
'23 AUG -9 A11 :45

Pursuant to Hawai'i Revised Statutes Section 92-3.7, which codified Act 220, SLH 2021, the meetings of the County of Kaua'i Historic Preservation Review Commission will be conducted as follows:

- **The meeting location that will be open to the public is:**

  Office of Boards and Commissions
  4444 Rice Street, Suite 300
  Līhu'e, HI 96766

- **Written testimony** indicating your 1) name or pseudonym, and if applicable, your position/title and organization you are representing, and 2) the agenda item that you are providing comment on, may be submitted on any agenda item in writing to planningdepartment@kauai.gov or mailed to the County of Kaua'i Planning Department, 4444 Rice Street, Suite 473, Līhu'e, Hawai'i 96766. Written testimony received by the Planning Department at least **24 hours prior** to the meeting will be posted as testimony to the Kaua'i Historic Preservation Review Commission's website prior to the meeting (https://www.kauai.gov/Government/Boards-and-Commissions/Historic-Preservation-Commission). Any testimony received after this time will be retained as part of the record, but we cannot assure the Commission will receive it with sufficient time for review prior to the meeting.

- **Oral testimony** will be taken on specific agenda items, **at the public meeting location** indicated on the meeting agenda.

- **IF YOU NEED AN AUXILIARY AID/SERVICE, OTHER ACCOMMODATION DUE TO A DISABILITY, OR AN INTERPRETER FOR NON-ENGLISH SPEAKING PERSONS, PLEASE CONTACT THE OFFICE OF BOARDS & COMMISSIONS AT (808) 241-4917 OR ADAVIS@KAUAI.GOV AS SOON AS POSSIBLE. REQUESTS MADE AS EARLY AS POSSIBLE WILL ALLOW ADEQUATE TIME TO FULFILL YOUR REQUEST. UPON REQUEST, THIS NOTICE IS AVAILABLE IN ALTERNATE FORMATS SUCH AS LARGE PRINT, BRAILLE, OR ELECTRONIC COPY.**

KAUA'I HISTORIC PRESERVATION REVIEW COMMISSION MEETING NOTICE AND AGENDA

'23 AUG -9 A11 :45

Thursday, August 17, 2023
1:30 p.m. or shortly thereafter
Līhu'e Civic Center, Office of Boards and Commissions
4444 Rice Street, Suite 300, Līhu'e, Kaua'i, Hawai'i

A. CALL TO ORDER BY CHAIR

B. ROLL CALL

C. APPROVAL OF AGENDA

D. APPROVAL OF THE MINUTES

a. October 6, 2022
b. October 20, 2022

E. GENERAL BUSINESS

F. COMMUNICATIONS

G. UNFINISHED BUSINESS

H. NEW BUSINESS

1. **The Church at Kōloa**
Proposed Additions to the Existing Historic Church
Property Address: 3251 Po'ipū Road/ 3269 Po'ipū Road
Tax Map Key: (4) 2-8-010:008
Kōloa, Hawai'i

Consideration of a zoning permit for proposed additions to an existing historic church building.

a. Director's Report pertaining to this matter.

I. EXECUTIVE SESSION:
Pursuant to Hawai'i Revised Statutes Sections 92-4 and 92-5(a)(4), the purpose of this executive session is to consult with the County's legal counsel on questions, issues, status and procedural matters. This consultation involves consideration of the powers, duties, privileges, immunities, and/or liabilities of the Commission and the County as they relate to the following matters:

1. **The Church at Kōloa**

Proposed Additions to the Existing Historic Church
Property Address: 3251 Po'ipū Road/ 3269 Po'ipū Road/
Tax Map Key: (4) 2-8-010:008
Kōloa, Hawai'i

Consideration of a zoning permit for proposed additions to an existing historic church building.

a. Director's Report pertaining to this matter.

K. ANNOUNCEMENTS

a. Charter Review Commission Proposal Request

L. SELECTION OF NEXT MEETING DATE AND AGENDA TOPICS (September 21, 2023)

M. ADJOURNMENT

COUNTY OF KAUA'I
Minutes of Meeting
SPECIAL OPEN SESSION

DRAFT To Be Approved

Board/Commission:	**Kaua'i Historic Preservation Review Commission**	Meeting Date	**October 6, 2022**
Location	Kōloa Neighborhood Center, 3461 Weliweli Road, Kōloa 96756,	Start of Meeting: 1:31 p.m.	End of Meeting: 3:51 p.m.
Present	Vice Chair Stephen Long. Commissioners: James Guerber, Gerald Ida, Susan Remoaldo and Aubrey Summers. Deputy County Attorney Stephen Hall. Planning Department Staff: Director Ka'āina Hull, Deputy Director Jodi Higuchi Sayegusa, Planner Marisa Valenciano, Planning Program Manager Myles Hironaka, and Planning Commission Secretary Shanlee Jiminez. Office of Boards and Commissions: Administrator Ellen Ching, and Commission Support Clerk Arleen Kuwamura.		
Excused	Chair Carolyn Larson and Commission Support Clerk Sandra Muragin		
Absent			

SUBJECT	DISCUSSION	ACTION
A. Call To Order	Chair Pro Tem Long called the meeting to order at 1:31 p.m.	
B. Roll Call	Deputy Director Jodi Higuchi Sayegusa verified attendance by roll call and requested a verbal response; Commissioner Guerber replied here. Commissioner Ida replied here. Commissioner Remoaldo replied here. Commissioner Summers replied here. Vice Chair Long replied here. Chair Larson was excused.	Quorum was established with five commissioners present.
C. Approval of the Agenda		Ms. Summers moved to approve the October 6, 2022 agenda, as circulated. Ms. Remoaldo seconded the motion. Motion carried 5:0.
D. Approval of the Minutes	1. None for this meeting Ms. Higuchi Sayegusa informed the commission there were no minutes to approve and moved on to the next agenda item.	

D.a.
AUG 17 2023

SUBJECT	DISCUSSION	ACTION
E. General Business	1. Commission Site Visit to Sueoka Market at 5392 Kōloa Road. Ms. Higuchi Sayegusa explained the agenda was setup for the commission and public to walk and view the site area and return to the neighborhood center for discussion and questions. She outlined the following; • The meeting would be recessed before leaving to view the site. • The commission and public would leave the Kōloa Neighborhood Center by foot at approximately 1:45 p.m. and proceed to Sueoka Market, 5392 Kōloa Road. • Commissioners were not allowed to discuss or ask questions to each other or to the architect during the site visit. • Public discussion/testimony/questions to the commissioners or architects would not be taken during the site visit. • Public testimony would be received and discussed after the site visit when the meeting reconvened at the Kōloa Neighborhood Center. • The public may submit written testimony and/or comments pursuant to the instructions specified on the publicly noticed agenda. • The site visit may involve adjustments subject to weather conditions. • Transportation would not be provided. <u>ADM Architects Grant Sumile and Robyn Pila presented a power point presentation;</u> • The purchase between ABC stores and Sueoka Store included an agreement to preserve the name, continue to offer unique local goods sold in the store and preserve the snack shop menu and recipes. • The entire store front was under the National Historic Register. • The refrigeration and air conditioning equipment area were not deemed historic and would be demolished. • Showed proposed site plan of the existing property and the area where the new two-story storage building would be constructed to consolidate and organize the numerous storage containers on the property. • Existing unoccupied residential home would be demolished and become a vacant grassy area. Future plans may include the construction of a one-story building for possible office	

SUBJECT	DISCUSSION	ACTION
	rental use. • Showed proposed site plan with improvements over the existing buildings. Per KHPRC recommendations they agreed to keep the large mango (*should be lychee*) tree and adjusted the road and storage for better flow. • Showed site plan of the existing driveway, which would be kept the same. Front stalls would be removed, and the main parking area would be relocated to the back. • New front entrance would be next to the new covered lanai area in the back. • Open a blocked side road, as another access to the property. <u>Public Testimony:</u> 1. Public person asked which road was being unblocked. Mr. Sumile replied it was the Makai Road, which ran parallel to the other back road. Makai road was gated, and they plan to open it for better flow. 2. Public person asked Mr. Sumile to point out where they plan to relocate the main parking. Mr. Sumile said in the back area. 3. Public person asked if there would be front parking. Mr. Sumile replied there would be parking in the front and the front entrance would remain. There would be two entrances one was the original front entrance and the second was a new back entrance. 4. Tessie Kinneman stated a lot of people like the front parking to quickly grab and go and parking in the back was too far. Mr. Sumile showed a site plan with the front entry and parking along Waikomo stream. <u>ADM Architects Grant Sumile and Robyn Pila presented a power point presentation;</u> • Adding coffee, bakery, and deli inside the store with fresh salads and sushi. • The front portion of the store would be preserved. <u>Public Testimony:</u> 5. Tessie Kinneman inquired about handicap parking. Mr. Sumile replied it was located by the new store entrance in the back. 6. Tessie Kinneman asked if the traffic flow would be one-way. Mr. Sumile replied two-ways.	

SUBJECT	DISCUSSION	ACTION
	7. Koa Young asked if they could enter the parking lot through the back way. Mr. Sumile replied yes, the current back road used now would become the loading/unloading area and pointed to the three entrances onto the property. 8. Koa Young stated the Kōloa Road crosswalk was right in front of the Sueoka Store entrance. He asked if they planned to reposition the sidewalk. Mr. Sumile replied the entrance and sidewalk would remain the same. 9. Anna Modez asked for clarification. She asked if Mr. Sumile represented the owners, ABC Stores and if he was asking planning commission permission for the expansion. Several commissioners responded yes but it was Kaua'i Historic Preservation Review Commission not planning commission. 10. Anna Modez asked if this was the first step and if it would then go to the planning commission. Ms. Higuchi Sayegusa explained this commission reviewed proposals with historic properties and Sueoka Store was on the state and national historic register. Because of this designation it was required to come before KHPRC for input on proposals to mitigate any impacts on historic properties. Ms. Modez appreciated the process and that the store front would remain. Her concern was with the design with the back area which looked too modern and mimicked the Kīlauea shopping mall expansion look. She recommended a redesign to incorporate more of the original small Koloa town feel. 11. Anna Modez asked if they could redesign or was this a final design. Ms. Higuchi Sayegusa said this was for testimony and they would do a site visit and go through more discussion and decision making. Ms. Modez said its an aesthetic concern. Mr. Sumile explained the national historic register guidelines don't want improvements to replicate what was there it should differentiate from the original. Ms. Modez asked if there was a possibility to change the design at this stage. Ms. Higuchi Sayegusa replied yes and that was what this process was about. 12. Anna Modez commented she appreciated accommodating the mango (*should be lychee*) tree. 13. Elizabeth Okinaka stated she was not a fan of the second entrance and the design looked like a new market. She liked the original one entrance and did not like the two entrances. She commented about accepting changes but hoped Sueoka store would remain the same and have the same small Kōloa town feel.	

SUBJECT	DISCUSSION	ACTION
	14. Jeri DiPietro of Kōloa Community Association commented the windows should not be metal. Commissioner Questions: 1. Chair Pro Tem Long stated the primary issue was the scale of the two-story storage building in the back. He asked for the square footage of the original storage and the square footage of the new two-story storage. Mr. Sumile replied the new one was larger to accommodate a generator and larger walk-in coolers and freezers. 2. Chair Pro Tem Long asked for the height of the existing Sueoka Store and the height of the new storage structure. Ms. Summers replied the sections showed the heights. Deputy County Attorney Stephen Hall announced that during the site visit the commissioners were not able to talk amongst each other or ask questions. At the site, the applicant, Mr. Sumile, would present and point out the information he talked about but there would be no interaction from the commission and asked the public to also not interact with the applicant or commissioners. Public Testimony: 15. Sandra Matsumoto stated she didn't see any solar panels and asked if it was restricted because of the historic designation. Mr. Sumile said there were solar panels on the roof now and they were planning to increase it. 16. Sandra Matsumoto asked that the new entrance red wall the bottom part of the storage if there was a way to make it look friendly. Mr. Sumile replied it would have landscaping in front of the wall. Ms. Matsumoto said it feels blocked in and not friendly looking. 17. Anna Modez asked if there was any way to shorten the red storage structure due to the incoming back entry lane. Cars parked in the stall would have limited view of the and back out into traffic. Mr. Sumile replied he would investigate. The best area to put the storage was in the back. Ms. Higuchi Sayegusa asked if they could proceed with the site visit and then return to continue the questions.	

SUBJECT	DISCUSSION	ACTION
	Chair Pro Tem Long announced the meeting would temporarily be relocated to the Sueoka Market site. *The commissions site visit to Sueoka Market started at 2:26 p.m.* Mr. Sumile addressed the following along the site visit; • Front – Front area will be preserved. Kiosk part of property will be removed. The jalousie, wood and rock wall will be preserved. • Windows will be made of wood. • Briefly toured the inside of the store. Mural viewed as historic will be restored done by one of the Sueoka's friends. Ceiling surface mount lights will stay the same. • Snack shop window will remain. Expanding deli. Walk in cooler not historic, pushed out storage. First two stalls removed and parking along river all the way to the back. Physically stood in the expanded side of the deli. • Pointed out where the back of store would end. Pointed out the area of the lanai. Pointed out the large two-story storage. • Driveway pointed out end of storage building loading zone and where the area of the parking stalls by the back entrance. • Pointed out which storage sheds would be eliminated. • Pointed out the mango tree, corrected to lychee tree would remain. • Pointed out the back road that goes to the back parking area. • Pointed out the edge of the storage building • Pointed out the loading zone area • Pointed out the area of the storage building • Pointed out the residential house – remove and grass the area • Generator would be placed in the grass area • Existing structure would remain and pointed out the expansion roofline and storage roofline • Pave back parking area • Pointed out the other road by the existing lychee tree	

SUBJECT	DISCUSSION	ACTION
	Mr. Sumile concluded the site visit and the group returned to the Kōloa Neighborhood Center. *The commission returned from the site visit at 2:47 p.m.*	
F. Communications	1. None for this meeting	
G. Unfinished Business (For Action)	**G.1. SMK Inc. (ABC Stores)** **Sueoka Market** **Demolition of Accessory Structure and Expansion of the Retail Store** Property Address: 5392 Kōloa Road Tax Map Key: (4) 2-8-008:020; (4) 2-8-008:022; (4) 2-8-0087:023; (4) 2-8-008:024; (4) 2-8-008:025; (4) 2-8-008:026; (4) 2-8-008:027; (4) 2-8-008:028; (4) 2-8-008:029; (4) 2-8-008:034; (4) 2-8-008:035, Yamada Road and River Road Kōloa, Hawai'i Consideration of a Class I Zoning Permit for the purposed demolition of accessory structures and the proposed expansion of the retail store. Chair Pro Tem Long called the meeting back to order. Chair Pro Tem Long announced that they would start with public testimony and asked that they state their name and refer their questions to Architect Grant Sumile or the commission. <u>Public Testimony:</u> 18. Tessie Kinnaman said back in 2006 Architect Lloyd Sako designed a two-story building, but it was not for storage. Mr. Sumile replied that was a previous architect and not part of them. 19. Tessie Kinnaman asked about the cultural study. Mr. Sumile replied an environmental assessment started and they plan to submit for review in January. 20. Tessie Kinnaman asked if the storage by the lychee tree would be gone. Mr. Sumile replied yes.	

SUBJECT	DISCUSSION	ACTION
	21. Tessie Kinnaman asked about the wastewater hookup. Mr. Sumile replied yes it was happening in the community. Chair Pro Tem Long asked Mr. Sumile to display his power point presentation. <u>Public Testimony:</u> 22. Anna Modez appreciated the site visit and said the storage lined up next to the road and lychee tree and the parking stalls next to the storage would be a problem. She advised for safety reasons that they reduce another six feet of storage space because cars backing out had no sight line and could back out onto incoming traffic. Mr. Sumile replied the road was wide enough for three lanes and they could stripe a two-lane road further away from the storage shed. Ms. Modez recommended they change the flat roof design to a more accessible viewing with 2x4 like ceiling or shaped up with fans. 23. Elizabeth Okinaka asked about the current back entrance and how accessible it would be and was concerned that it could be blocked off by storage containers. Mr. Sumile said there were not many choices to place the storage building but there would still be access. Ms. Okinaka asked if the home would be gone. Mr. Sumile said yes. Ms. Okinaka expressed disappointment in having an old plantation home demolished. 24. Jeri P. Peatro asked if the home could be relocated to the Koloa Rum site and said the area lacked tables and benches to eat. Mr. Sumile said there would be benches and tables in the front and in the grass area. Mr. Peatro asked if once the office area was built would it have its own parking, due to the lack of parking now. Mr. Sumile stated the number of parking stalls was over the required amount and would talk with ABC on preserving the house. 25. Koa Young expressed concerns about the old house and hoped they would renovate and rent to a local family. With no further testimony or comments from the public, Chair Pro Tem Long closed public testimony and announced the commission now had an opportunity to question Mr. Sumile after Marisa Valenciano completed the directors report.	

SUBJECT	DISCUSSION	ACTION
	Planner Marisa Valenciano shared the following; • Sueoka store was on the National and State Historic Register and by law KHPRC had the ability to review this project. • This project would not go to the planning commission. • The Owners and Architect want to do the right thing for Sueoka store. • The department had been in discussion with the owner and architect since July and the public could access that information online. • The department recommended to support with six conditions; 1) Compliant with secretary of interior standards 2) Applicant cognizant of HRS (Hawai'i Revised Statutes) 6010 review process 3) Applicant comply with any EA (Environmental Assessment) requirements 4) Prior to demolition permit provide photos of all structures scheduled for demolition 5) Applicant ensure additional mitigation measurements implemented prior to and during demolition. 6) Applicant consider paint palette consistent with old Kōloa town historic buildings 7) #7 not necessary, eliminate. • In addition, Ms. Valenciano added the commission consider comments from HHF (Hawai'i Historic Foundation) <u>Commissioner Questions:</u> 1. Mr. Guerber asked if there were 70 parking stalls. Mr. Sumile replied yes and with the square footage only 39 were required. 2. Mr. Guerber asked for a total square footage of the demolished buildings and the square footage of the replacement buildings. Mr. Sumile replied it was a smaller footprint relative to the size of the lot. Mr. Sumile asked if they could provide an answer in a follow up correspondence.	

SUBJECT	DISCUSSION	ACTION
	Public Testimony: 26. Anna Modez stated this was not going to the planning commission and asked if there was going to be a follow-up meeting to see if the design was implemented. Ms. Valenciano said the commission would decide if that was necessary. The department was comfortable enough to support the project along with the public's comments. Ms. Modez said it was the first time the community was aware of this project and based on the public testimony they share the same concerns regarding keeping the house and the façade of the extension design. She wanted assurance that the owner and architect implement their suggestions into the design plans. 27. Elizabeth Okinaka requested to be informed of the EIS (Environmental Impact Statement). 28. Tessie Kinnaman was concerned that construction would dig up lava tubes and requested they not block or fill the lava tubes. 29. Tessie Kinnaman asked for a timeline. Mr. Sumile replied that if the EA is completed in January they would submit permits in late February early March and start construction (*inaudible*) or early next year. 30. Tessie Kinnaman commented it was nice to have more parking stalls than required but was concerned that it may lead to construction of additional buildings in the future. Commissioner Questions: 3. Ms. Remoaldo asked if the lava rocks was going to be salvaged and reused. Mr. Sumile replied they have some of it. 4. Ms. Remoaldo said there was a lava rock piled up in the parking area and some low level lava rock walls were dismantled. She asked that these lava rocks be salvaged and reused. 5. Ms. Remoaldo stated that page three of the preservation and expansion handout the outdoor lanai had wooden slat windows and on another page the storage building had louvered windows. She asked if these would be the same wooden windows. Mr. Sumile replied yes the windows would match and be wooden. 6. Ms. Romoaldo asked if the store front jalousies would remain the same. Mr. Sumile replied yes it would. 7. Ms. Remoaldo asked that they consider the type of landscaping plants to use because the public may harvest it for themselves. She also reminded Mr. Sumile that native plants was	

SUBJECT	DISCUSSION	ACTION
	mentioned for use in the landscaping. 8. Ms. Remoaldo stated during the site visit she recognized a vintage world war II landing mat on the ground and asked that if they encounter other interesting artifacts on the property during demolition that it be preserved and displayed. Mr. Sumile said workers have mentioned that some of the storage containers have old signs and fixtures. 9. Ms. Remoaldo said she suggested at the last meeting that the lanai wall be used to tell the story of Sueoka. Mr. Sumile said yes the owners liked the idea 10. Mr. Ida recalled that they talked about the old house and remembered that the structure would be replaced at a later time and not developed the same time. Mr. Sumile replied yes. 11. Mr. Ida said the condition of the home wasn't too bad and recommended they explore the possibility to reuse or give it to someone who would be willing to transport it off property. Mr. Sumile replied that ABC had approached this project with the best spirit possible and with honest intentions of preserving the integrity and uniqueness of the property. He plans to share with the owner the comments to restore and repurpose the home as well as the other comments about the back entrance and shrinking the storage size and compromise and come up with a reasonable solution. 12. Chair Pro Tem Long asked for the height of the existing Sueoka store and height of new storage structure. Architect Robyn Pila replied according to page 14 the height of the new two-story storage was 28' 7" and store front was around 28' but was higher than the roof pitch. Ms. Pila explained that the land sloped two feet from the front to the back lowering the height of the roof. Ms. Summers asked if Chair Pro Tem Long was inquiring about the front façade or the roof and he replied the peak. Ms. Summers stated the front façade was 28' and the roof height was lower. Chair Pro Tem Long asked for the height of the roof and Ms. Pila replied the height of the roof interior was 23'. Chair Pro Tem Long asked for the top of the ridge height and Ms. Summers replied 24'. Chair Pro Tem Long stated the new structure was 4' 7" higher and Ms. Summers replied it was the same as the front façade. Chair Pro Tem Long stated he referred to the roof ridge and they had a difference of 4'7". 13. Chair Pro Tem Long asked floor to ceiling height of the first and second floor of the new storage building. Mr. Sumile replied 10' on the ground level and 8'6" on the second floor. Chair Pro Tem Long asked if there was a functional reason why the	

SUBJECT	DISCUSSION	ACTION
	ground floor needed to be 10'high. Mr. Sumile replied yes it was volume, it enabled them to stock more inventory higher as opposed to wider. 14. Chair Pro Tem Long stated his comments and concerns on the mass and scale of the new two-story storage building was not mentioned and that it was out of place in old Kōloa Town. He reiterated his comments to reduce the scale and mass of the storage units flat wall and that greater effort be done architecturally to reduce it. 15. Ms. Summers commented that professionally the new storage building was like an old building and reinterprets the existing building. The new two-story storage mass was very similar to what was there now with the flat wall and no windows. She was confused because one set of conversation wanted to preserve the look and feel of the old buildings and another set of conversation wanted to pretty up the large scale of the flat wall. With no further comments or questions from the commissioners, Chair Pro Tem Long asked the commission to either approve the plans as presented or ask for deferral to get additional information.	Mr. Guerber moved to defer action on the SMK Inc. (ABC Stores) Sueoka Market Demolition of Accessory Structure and Expansion of the Retail Store. Property Address: 5392 Kōloa Road, Tax Map Key: (4) 2-8-008:020; (4) 2-8-008:022; (4) 2-8-0087:023; (4) 2-8-008:024; (4) 2-8-008:025; (4) 2-8-008:026; (4) 2-8-008:027; (4) 2-8-008:028; (4) 2-8-008:029; (4) 2-8-008:034; (4) 2-8-008:035, Yamada Road and River Road, Kōloa, Hawai'i Sueoka Store application until a future

SUBJECT	DISCUSSION	ACTION
		meeting. Mr. Ida seconded the motion. (*motion died with no vote*)
	Ms. Higuchi Sayegusa said there were timelines for zoning permits statutes and ordinance and asked the commission to specify either October 20 or November 17 as the meeting date. Chair Pro Tem Long asked Mr. Sumile if he could have the designs ready by the next meeting. Mr. Sumile said ABC wants to preserve the store, but it needed to be an operatable and sustainable business. He said in one hand they were asking for more detail and also wanting to simplify and preserve the old. Mr. Sumile would convey the concerns to the owner, but the storage needed to be feasible and work for the business to be profitable. <u>Public Testimony</u>: 31. Koa Young stated that another architectural design that would make the large size of the storage seamless could be the use of white trim with red. Attorney Hall requested the commission identify a meeting date of October 20 or November 17 in the motion due to permit timelines. Ms. Higuchi Sayegusa stated the house would not be included in the demotion permit and would be discussed at a later time. This was just for the store renovation. <u>Commissioner Questions:</u> 16. Mr. Guerber inquired on the age of the house. Mr. Sumile said it was over 50 years old. 17. Mr. Ida asked if the home was on the National Historic Register. Ms. Valenciano wasn't sure but would check the listing. 18. Ms. Summers asked when the store was purchased was the house written in the deed. She stated that if ABC sold the property to another owner the new owner could tear down the home. Mr. Sumile replied yes, they could. Mr. Sumile stated there was an agreement with Sueoka's and Paul Kosasa before the purchase to keep the old feel of the property and not demolish and rebuild a new structure. He said the storage was placed in the best possible area, tucked away, and provided ample traffic flow and parking. The two-story building was a better alternative to a single story that would be wider and	

SUBJECT	DISCUSSION	ACTION
	larger and take up more road and parking space. Mr. Sumile stated he could make it for the November 17 meeting.	Mr. Guerber moved to defer action on the SMK Inc. (ABC Stores) Sueoka Market Demolition of Accessory Structure and Expansion of the Retail Store. Property Address: 5392 Kōloa Road, Tax Map Key: (4) 2-8-008:020; (4) 2-8-008:022; (4) 2-8-0087:023; (4) 2-8-008:024; (4) 2-8-008:025; (4) 2-8-008:026; (4) 2-8-008:027; (4) 2-8-008:028; (4) 2-8-008:029; (4) 2-8-008:034; (4) 2-8-008:035, Yamada Road and River Road, Kōloa, Hawai'i Sueoka Store application until the November 17, 2023 meeting. Mr. Ida seconded the motion. Roll Call Vote: Mr. Guerber – Aye Mr. Ida – Aye Ms. Remoaldo - Aye Ms. Summers - Aye Vice Chair Long – Aye Motion carried 5:0
H. New Business	1. None for this meeting	

SUBJECT	DISCUSSION	ACTION
I. Executive Session	DCA Hall said there was no legal basis to enter executive session. The commission did not enter into executive session. 1. Commission Site Visit to Sueoka Market at 5392 Kōloa Road. **2. SMK Inc. (ABC Stores)** **Sueoka Market** **Demolition of Accessory Structure and Expansion of the Retail Store** Property Address: 5392 Kōloa Road Tax Map Key: (4) 2-8-008:020; (4) 2-8-008:022; (4) 2-8-0087:023; (4) 2-8-008:024; (4) 2-8-008:025; (4) 2-8-008:026; (4) 2-8-008:027; (4) 2-8-008:028; (4) 2-8-008:029; (4) 2-8-008:034; (4) 2-8-008:035, Yamada Road and River Road Kōloa, Hawai'i Consideration of a Class I Zoning Permit for the purposed demolition of accessory structures and the proposed expansion of the retail store.	
J. Announcements	Ms. Higuchi Sayegusa announced the following; • October 20, regular commission meeting at the Līhu'e Civic Center. • November 17, regular commission meeting at the Līhu'e Civic Center.	
K. Selection of Next Meeting Date and Agenda Topics (October 20, 2022 Regular Meeting)	Next meeting was scheduled for Thursday, October 20, 2022 Regular Meeting	
L. Adjournment	With no further business to conduct, Chair Pro Tem Long called for a motion to adjourn.	Ms. Remoaldo moved to adjourn the meeting. Mr. Ida seconded the motion. Motion carried 5:0.

SUBJECT	DISCUSSION	ACTION
		Chair Pro Tem Long adjourned the meeting at 3:51 p.m.

Submitted by: _____ Reviewed and Approved by: _____
Sandra M. Muragin, Commission Support Clerk Stephen Long, Chair Pro Tem

( ) Approved as circulated.
( ) Approved with amendments. See minutes of _____ meeting.

COUNTY OF KAUA'I
Minutes of Meeting
OPEN SESSION

DRAFT To Be Approved

Board/Commission:	**Kaua'i Historic Preservation Review Commission**	Meeting Date	**October 20, 2022**
Location	Mo'ikeha 2A/2B with remote access by Zoom Teleconference and Audio Connection	Start of Meeting: 1:29 p.m.	End of Meeting: 3:27 p.m.
Present	Chair Carolyn Larson. Vice Chair Stephen Long. Commissioners: James Guerber, Gerald Ida, Susan Remoaldo and Aubrey Summers (*attended by Zoom*). Deputy County Attorney Stephen Hall (*attended by Zoom*). Planning Department Staff: Director Ka'āina Hull (*arrived at 1:33pm and left at 2:46pm*), Deputy Director Jodi Higuchi Sayegusa Planner Marisa Valenciano, Planner Myles Hironaka (*attended by Zoom*), and Commission Support Clerk Duke Nakamatsu. Office of Boards and Commissions: Administrator Ellen Ching, and Commission Support Clerk Arleen Kuwamura.		
Excused	Commission Support Clerk Sandra Muragin		
Absent			

SUBJECT	DISCUSSION	ACTION
A. Call To Order	Chair Larson called the meeting to order at 1:29 p.m.	
B. Roll Call	Deputy Director Jodi Higuchi Sayegusa verified attendance by roll call and requested a verbal response; Commissioner Guerber replied here. Commissioner Ida replied here. Commissioner Remoaldo replied here. Commissioner Summers replied here. Vice Chair Long replied here. Chair Larson replied here.	Quorum was established with six commissioners present.
C. Approval of the Agenda		Mr. Guerber moved to approve the October 20, 2022 agenda, as circulated. Ms. Remoaldo seconded the motion. Motion carried 6:0.
D. Approval of the Minutes	1. June 16, 2022	Ms. Remoaldo moved to approve the June 16, 2022;

D.b.

AUG 17 2023

SUBJECT	DISCUSSION	ACTION
	Ms. Remoaldo requested page 5, second bullet, meat pre area change to meat prep area. Chair Larson requested page 6, second bullet, various roof pitch change to various roof pitches. Chair Larson requested page 7, fourth bullet, recuse themselves to recuses themselves.	minutes as circulated. Mr. Ida seconded the motion. Chair Larson called for a vote to approve the amended June 16, 2022, minutes with a correction on page 5, "meat pre area" to "meat prep area; page 6, "various roof pitch" to "various roof pitches" and page 7, "recuse themselves" to "recuses themselves". Motion carried 6:0.
E. General Business	Ms. Higuchi Sayegusa said there were no general business.	
F. Communications	a. Email Memorandum and revised plans from ADM Architecture + Interiors dated October 11, 2022 to transmit the revised preliminary plans for Sueoka Market for the commission to review in advance of a future meeting. Ms. Higuchi Sayegusa said the memorandum from Architect Grant Sumile was a mockup that incorporated the discussions and comments that took place at the site visit, and it was not an action item.	Mr. Guerber moved to receive the memorandum and revised plans from ADM Architecture + Interiors dated October 11, 2022 to transmit revised preliminary plans for Sueoka Market for the commission to review in advance of a future meeting. Ms. Remoaldo seconded the motion. Motion carried 6:0

SUBJECT	DISCUSSION	ACTION
G. Unfinished Business	**G.1. Gay & Robinson, Inc. – Kaumakani Avenue** **Proposed demolition and proposed reconstruction of two existing single-family residences** **Tax Map Key: (4) 1-7-006:001** Consideration of a Class I Zoning Permit for the proposed demolition and the proposed reconstruction of two existing single-family homes located within the Kaumakani Avenue. Ms. Higuchi Sayegusa asked if anyone in the audience wanted to testify on this agenda item, hearing none Planner Myles Hironaka confirmed there were no public attendees online. Planner Marisa Valenciano stated at the August 18, 2022, meeting the commission approved demolition and requested the applicant to return for the window update. She called up Director Ka'aina Hull to share his discovery with the commission. Mr. Hull updated the commission on their meeting with building division to inquire about the possibility to preserve and use the historic windows. To their surprise they learned of an exemption from building code standards that was permitted by building division. Unbeknownst to them the exemption could be obtained with the following conditions; the structure must be deemed historic, and it must undergo a full preservation and restoration of the structure. What that meant was the structure would need to be repaired and reconstructed in the original method which included single wall construction, preservation of windows, utilization of the floors and retrofits, the entire structure would be a historic preservation project which included use of same materials. Mr. Hull asked the commission to be aware that most of the structures in this project were unable to be repaired and the applicant proposed demolition. Chair Larson said these structures could use the exemption and do a full restoration. Vice Chair Long replied cost would be a major factor and Mr. Hull added that acquiring skilled services to perform the restoration would be another factor. Vice Chair Long said they did not have the August meeting minutes to reference and he clearly remembered the applicant wanted to replicate the structures as closely as possible to the existing structures. The word "replicate" was used by the applicant which gave him hope of the	

SUBJECT	DISCUSSION	ACTION
	applicant's commitment to replicate the structures original features. Chair Larson remembered the word "replicate" also but recalled that they were not planning to use the same type of windows and doors. Chair Larson stated the commission accepts this project with the condition that they replicate the windows and doors as close as possible to the original. Mr. Guerber commented that Waimea Plantation Gardens reused old single wall plantation homes and he encouraged the use of single walls in these structures. Ms. Summers stated there was a conflict with some of the commissioners in their single wall construction comments. Since the applicant planned to demolish the structure and rebuild it would be considered new construction and single wall construction would not be required. Gay & Robinson, Inc. Real Estate Director Koa Duncan acknowledged the commissions concerns to "replicate" and stated they would like to move forward with their plans to demolish and rebuild to the form and character of the existing structures. The new windows would match as close as possible to the original. Gay & Robinson, Inc. Vice President Howard Green (*attended by Zoom*) added that the doors would have indentions and trim to match a plantation style. Plain flat doors would not be used. Mr. Duncan passed out a color photo of Kaumakani eight homes that the commission approved in the past. (*An electronic copy was emailed to Commissioner Summers*). The homes were demolished and rebuilt to closely match the original. Vice Chair Long didn't understand why they were given copies to view when the windows installed in the photo were not historical. Mr. Green explained that the vinyl windows closely matched the original double hung windows. Chair Larson reiterated the commission's request for the windows and doors to closely match the original look and encouraged the applicant to seek sources that could produce these products. She stated windows and doors made a difference visually and it was important to restore since the structures were on Kaumakani's main avenue.	

SUBJECT	DISCUSSION	ACTION
	DCA Stephen Hall briefly highlighted the commissions comments as followings: • Vice Chair Long commented on replicating windows and doors to closely match original. • Mr. Guerber commented on use of single wall construction. • Chair Larson commented on keeping the character of the windows and doors and different from vinyl windows. Chair Larson added that the commission ruled out on the use of single wall construction. Ms. Higuchi Sayegusa stated these comments would be used to advise the department to consider when issuing a building or zoning permit and could be added as a suggestion or recommendation. Mr. Guerber asked if the buildings were termite infested and once demolished it allowed the applicant to build what they want. Ms. Higuchi Sayegusa replied yes, this was an opportunity for the applicant to hear the concerns from the commission but in the end the applicant could proceed with their plans; however, they expressed their willingness to restore with the commissions suggestions as much as possible. Mr. Guerber addressed the applicants and said they understood the commissions strong concerns and hope they take their comments into consideration. Chair Larson recommended to amend the motion and include the condition that replacement windows and doors be wooden and match closely to the original.	Vice Chair Long motioned to support the applicant and their representation before the commission that they would like to replicate these historical buildings. Mr. Guerber seconded the motion. (*motion died no vote*) Vice Chair Long motioned to amend the original motion and include the condition that replacement windows and doors be wooden and match closely to the original. Mr. Guerber seconded the motion. (*motion died no vote*)

SUBJECT	DISCUSSION	ACTION
	Mr. Hull added that this application must be reviewed and acted on by the department to meet specific deadlines and timelines. Once a zoning permit application is submitted its reviewed within the deadlines or its automatically approved. The applicant expressed willingness to work with the commission but was also held to these specific deadlines and timelines. For this reason, the applicant may not have a chance to return and present their proposed reconstruction before the commission.	Vice Chair Long motioned that the applicant present KHPRC in the future with proposed plans and elevations of the homes that they plan to rebuild that meet current building codes such that could not be replicated which would be reconstruction as closely as possible to the historic house as it existed now and in particular emphasis on true divided light double hung wood windows, accurate historical doors and any other materials and finishes on the exterior that support that motion and also recognizing that the applicant would like to revise the interior floor plan layout that KHPRC supports and that the applicant comes before KHPRC at a future meeting to present their proposed reconstruction. Mr. Guerber seconded the motion. Motion carried 5:1 (*Summers-Nay*)

SUBJECT	DISCUSSION	ACTION
	Vice Chair Long replied that he was informed by the department's staff that this was a preliminary presentation, and a building permit was not submitted. He confessed he was not familiar with the departments timeline and asked if the applicant would agree to return at a future meeting. Ms. Higuchi Sayegusa suggested it might be helpful to amend the motion and insert direction and specifications, instead of requesting that the applicant return. Mr. Hull stated that Ms. Valenciano worked closely with applicants when a zoning permit is submitted. He said there are applicants who could choose to not consider all the recommendations of this commission but added he was not talking about this applicant. Due to the strict zoning permit deadlines the applicant may not return for the commission to review. Vice Chair Long replied he understood and in his opinion the department had not received an acceptable accurate application and the applicant should not be in any deadline. Mr. Hull replied that it was not the responsibility, and this commission did not have the authority to advise the department whether a permit application was acceptable or accurate. Mr. Hull reiterated the 21-day deadline the department had to review applications. Vice Chair Long replied that this commission voted and approved an acceptable application would include accurate and complete before and proposed floor plans, exterior elevations and materials, finishes, color schedule and that information has not been provided to the commission today. Chair Larson stated the motion could be revised to include these conditions. Vice Chair Long said in addition to the proposal made he wanted to add that specific attention be given to the doors, windows, siding, and color. DCA Hall advised that the commission do a "motion to reconsider" the last motion that passed and then make a new motion. Mr. Greene commented that Mr. Duncan handed out pictures of a successful project that KHPRC approved in the past. He said the Kaumakani avenue was an asset, and they want to preserve that historic place and keep it beautiful. *Chair Larson called for a five-minute recess at 2:32 p.m.* *Chair Larson called the meeting back to order at 2:37 p.m.*	

SUBJECT	DISCUSSION	ACTION
	Mr. Greene continued that working with single wall construction and procuring materials to original specifications was difficult and made it cost prohibited. They want to make a safe home with modern living standards, energy efficient and would try to maintain the historical nature of the avenue.	Mr. Guerber moved to reconsider Vice Chair Longs motion. Vice Chair Long seconded the motion. Motion carried 6:0. The committee voted again on Vice Chair Longs original motion. Motion failed 0:6. Vice Chair Long moved that the applicant reconstructs these historic homes as close as possible to the existing original home as is that they are going to demolish and specific attention be given to installing true divided light wood double hung windows, doors as closely representative of the existing and siding and color as close to existing. Mr. Guerber seconded the motion.
	Vice Chair Long commented that if the applicant adhered to the commissions comments they would not need to return to the commission. Chair Larson called for the vote. Ms. Summers explained her reason for voting against the motion was because she personally priced wood windows and the cost could prohibit the applicant from using it for this project.	Motion carried 5:1 (*Summers-Nay*)

SUBJECT	DISCUSSION	ACTION
H. New Business	**H.1. TRILEAF (on behalf of Verizon Wireless)** **Proposed installation of a new telecommunications facility on an existing rooftop at the Sheraton Kaua'i Coconut Beach Resort Hotel along with new ground equipment cabinets, underground utilities, and associated improvements** Sheraton Kaua'i Coconut Beach Resort Hotel 650 Aleka Loop, Kapa'a Tax Map Key: (4) 4-3-007:028 Kapa'a, Hawai'i National Historic Preservation Act, Section 106: Consultation with Native Hawaiian Organizations and Potential Consulting parties a. Director's report pertaining to this matter. Planner Marisa Valenciano read portions of the directors' report; • The commission's action for the project was to; 1.Provide comments for identification of cultural and historic resources. 2.Defer providing comments. 3.Provide comment of no comments • The department recommended the commission provide comments for the Section 106 letter. Ms. Higuchi Sayegusa stated there was no one from the public to testify and Mr. Hironaka stated no attendees raised their digital hand. Megan Austin (*entered by Zoom*) with Trileaf Corporation consulting firm responsible for Section 106 and Kathy O'Connor Phelps (*entered by Zoom*) who submitted permit application on behalf of Verizon did not have a presentation and other Verizon representatives were available to answer any questions. Ms. Phelps stated they provided a cultural report, no coconut trees would be removed, and they	

SUBJECT	DISCUSSION	ACTION
	would not move the equipment. Questions: • Mr. Ida asked if there was any archaeological study done specifically for this project. Ms. Austin replied yes. An SOI (Secretary of Interior) qualified archaeologist completed a cultural survey, and it was submitted to the State Historic Preservation Department for review. She stated the visual area of potential effect was outlined on page 5, of the cultural resource report and on page 52 of the SHPD (State of Hawai'i Historic Preservation Division) submittal package sent on October 14, 2023. SHPD has not responded back to them, they anticipate a response in a few weeks. • Mr. Ida asked if an archaeologist was on site. Ms. Austin replied yes. • Mr. Ida asked if there was any subsurface testing done. Ms. Austin replied no. • Mr. Ida asked if SHPD directed them to complete any follow-up study. Ms. Austin confirmed no shovel test kits were conducted on the site since it was the existing paved parking lot. • Chair Larson asked if they received any recommendations from SHPD. Ms. Austin replied no and since their application was sent on October 14, they anticipate a response around mid-November. • Vice Chair Long asked Mr. Ida if he had any concerns that sub-surface testing was not done. Mr. Ida replied yes, there should be subsurface investigation before the project starts. He stated his concerns were that there were burials close to the site of the project, burials to the north of the property and when the resort was built there were no state burial laws in place. • Chair Larson asked if this project was going to the arborist advisory committee. Ms. Higuchi Sayegusa replied probably not since no trees were going to be disturbed. Ms. Valenciano added the applicant was going to add a notation on the plans. Chair Larson stated the coconut grove was an historic property and asked the applicant if they would consider planting new trees in areas where there once were trees. Noah Bronson of Verizon stated the site plans noted that the trees would not be disturbed. Mr. Bronson reassured the commission that no trees were proposed to be removed and ground	

SUBJECT	DISCUSSION	ACTION
	equipment would be on the existing paved parking lot and antennas on the buildings roof. • Chair Larson asked if greenery was going to be added around the new unit that was going to be placed on the ground. Ms. Austin replied no, bollards would be placed around that area. • Mr. Ida asked Chair Larson if she said the coconut grove was a historic site. Chair Larson replied no, but if she did, what she meant was the historic grove itself was historic. Ms. Higuchi Sayegusa clarified that the grove was designated as an exceptional tree. Mr. Ida was concerned about the coconut grove which to him was not cultural but very historic. Ms. Higuchi Sayegusa said the exceptional tree designation did not prevent them from including comments in the Section 106 letter. Chair Larson said the grove was an essential feature of that community and crucial to the view and ambience in that area and represented the remainder of a larger grove that used to be there. She questioned the visual impact of the placement of the equipment on one side of the grove and suggested a green barrier between the equipment and the grove would be more appropriate. • Ms. Phelps asked if Chair Larson referred to the ground equipment. Chair Larson said it looked like the ground equipment would be placed right next to the grove. Ms. Phelps replied no, its more towards the beach. She said the area did not have the space to fit greenery because it had a beach access easement and was mostly concrete. She commented that adding greenery would not add to the area because it was in the back shipping area. Chair Larson summed up the discussion and said the commission had concerns with what was under the paved areas and Mr. Guerber added they were concerned with where they would trench. Ms. Phelps inserted a correction and said the access road placed on plans would not be trenched and the fiber and electrical trench would be behind the coconut trees, the trench would be about three feet wide. She confirmed no trenching in the parking lot. • Mr. Guerber asked how deep the trench would be. Ms. Phelps did not have that	

SUBJECT	DISCUSSION	ACTION
	information. Mr. Bronson did not have the information also but said it would be like a typical utility trench. Mr. Ida stated they did not have to dig very deep to uncover burials or cultural materials. Mr. Bronson replied that they could have someone on site to inspect during trenching. Ms. Phelps added that planning commission placed into their conditions of approval that archaeological cultural monitoring be required during all ground disturbing activities. • Ms. Remoaldo referred to page A04, showed the building and coconut trees and asked if it was existing coconut trees. Mr. Bronson replied yes, it was existing coconut trees. • Ms. Remoaldo asked if the drawings were accurate because the building was taller than the coconut trees. Mr. Bronson replied yes, that was accurate. Ms. Phelps added that they measured the diameter and height of each coconut tree. Ms. Remoaldo stated her concern was the visual impact the roof top antennas would have and the effect it would have on the ambience of the location. Mr. Bronson replied they were installing stealth antennas that would be located inside a structure that blended into the existing building. The antennas would not be visible. Ms. Phelps added that it was an extension of the existing stairwell. • Chair Larson stated it would increase the existing height of the building and asked for the original height of the building. Ms. Phelps referred to page A03. Mr. Bronson replied it would be a 10' increase. • Chair Larson asked how big the box was. Ms. Phelps said the dimensions were on A01, 9' wide by 29'7" across. Ms. Remoaldo suggested they hide the proposed equipment without it interfering with the area. Ms. Higuchi Sayegusa said they could recommend camouflaging the equipment with landscaping to blend into the surrounding environment. Ms. Remoaldo stated if the applicant is unable to add plants in the area, they could use potted plants. • Chair Larson asked the applicant for their suggestion to help with enhancing the visual aspect of the equipment so it could blend into the area. Mr. Bronson replied landscaping wouldn't be appropriate, but they could do a special fence concealing the equipment. They would work with the resort.	

SUBJECT	DISCUSSION	ACTION
	• Chair Larson asked if the issue was space. Mr. Bronson replied yes, they would be using smaller equipment to not take up so much room in the resort. Chair Larson asked if there were any comments. With no comments from the commission for the Section 106 letter they moved on to the next agenda item.	
I. Executive Session	**1. Gay & Robinson, Inc. – Kaumakani Avenue** **Proposed demolition and proposed reconstruction of two existing single-family residences** Tax Map Key: (4) 1-7-006:001 Consideration of a Class I Zoning Permit for the proposed demolition and proposed reconstruction of two existing single-family homes located within the Kaumakani Avenue. **2. TRILEAF (on behalf of Verizon Wireless)** **Proposed installation of a new telecommunications facility on an existing rooftop at the Sheraton Kaua'i Coconut Beach Resort Hotel along with new ground equipment cabinets, underground utilities, and associated improvements** Sheraton Kaua'i Coconut Beach Resort Hotel 650 Aleka Loop, Kapa'a Tax Map Key: (4) 4-3-007:028 Kapa'a, Hawai'i National Historic Preservation Act, Section 106: Consultation with Native Hawaiian Organizations and Potential Consulting parties a. Director's report pertaining to this matter. Ms. Higuchi Sayegusa stated both agenda items were completed and there was no need for any further discussions in executive session.	
J. Announcements	Ms. Valenciano announced the following; a. **Historic Hawai'i Foundation** **Hawai'i Preservation in Practice Training Seminar: Identifying & Documenting**	

SUBJECT	DISCUSSION	ACTION
	Character-Defining Features Wednesday, October 26, 2022 10:00am-11:30am Virtual Webinar via Zoon Ms. Higuchi Sayegusa said the October 26, seminar was live so commissioners would be able to ask questions. Advance registration was required. Ms. Higuchi Sayegusa shared that the National Historic Preservation would conduct an online training November 1-4, and the department would reach out to commissioners with more information, registration may be required. Ms. Valenciano notified the commission that the November 17, meeting would be the last meeting of the year, no meeting in December.	
K. Selection of Next Meeting Date and Agenda Topics	Next meeting was scheduled for 1:30 p.m. Thursday, November 17, 2022, Regular Meeting	
L. Adjournment	With no further business to conduct, Chair Larson called for a motion to adjourn.	Ms. Remoaldo moved to adjourn the meeting. Mr. Ida seconded the motion. Motion carried 6:0. Chair Larson adjourned the meeting at 3:27 p.m.

Submitted by: _____ Reviewed and Approved by: _____
Sandra M. Muragin, Commission Support Clerk Carolyn Larson, Chair

( ) Approved as circulated.
( ) Approved with amendments. See minutes of _____ meeting.

The Church At Koloa
Est. 1835
Koloa, Kauai, HI

Location: *3269 Poipu Road*
Koloa, Hawaii 96756

Phone: *(808) 742-9956*

DATE: July 4, 2023

SUBMITTED TO: PLANNING DEPARTMENT
COUNTY OF KAUAI
4444 RICE STREET, Suite A473
LIHUE, HAWAII 96766
(808) 241-4060

SUBJECT: PROPOSED NEW ADDITIONS TO
HISTORICAL CHURCH BUILDING
KOLOA, HAWAII 96756
TMK: 2-8-010:008-0000

ATTENTION: MARISA VALENCIANO
PLANNER

Ladies and Gentlemen:

My name is Nadine Begley, I am a member of the church and the authorized representative for the Board Members of the " THE CHURCH AT KOLOA".

We humbly ask for your considerations to the following proposed scope of work:

1	Approximately 130 s.f. two story RIGHT SIDE OF BUILDING with a 2nd story room to host our security surveillance operation.
2	Approximately 130 s.f. two story LEFT SIDE OF BUILDING to ADD and ADA BATHROOM FACILITY, on the 1st floor with using the upper floor space for storage.
3	ADDING 2 EMERGENCEY EXITS located on the Right side of worship hall and left side of worship hall

H.I.
AUG 17 2023

The reason for the additions are two part:

PART 1

Under the Security Guide of the U.S. Department of Homeland Security which provides real INCIDENT CASE STUDIES and DATA.
It also provides information on HOW TO DEVELOP A HOLISTIC APPROACH to SECURITY and how to develop this plan.
We have provided **EXHIBIT "A"** for your reference.
"MITIGATING ATTACKS ON HOUSES OF WORSHIP"
(Reference Chapter 5 Pages 63-70)

We have growing concerns too with the OPEN BORDER Policy allowing thousands of illegal immigrants, drug dealers and many dangerous people in to our country. Its just a matter of time these types will make their way through out the various parts of the United States.
We hope and pray this will not be the case in our future, but being PREPARED should always be the choice over being PASSIVE. Especially when it comes to protecting lives and property.

In the past and present, we have experienced Intruders, Homeless individuals sleeping at the church entrance and random strangers that we called the police department for their assistance. Some were confrontational.

At the rear property where we have Several rental units, many families with young children, and a Private Grave yard.
We have had consistent trespassing of Drug and Alcohol users coming on to our property by way of the Government Owned Road adjacent along side the Church Properties.
This is a serious concern we all share for the safety of those that reside on the church property.

PART 2

Back when this Church was built in 1837, ADA did not exist.
ADA (Americans with Disabilities Act) was signed into law on July 26, 1990.
However, although the churches are EXEMPT from Title III of the ADA this law is still VERY NECESSARY for today's use.
We have several members that are elders, or on a wheelchair or are physically impaired, that attend our services.
We do not have the interior space to create one to ADA Building standards so this is the reason we are humbly asking your permission to do so.

We also feel that having the addition on both sides create an aesthetic BALANCE to the exterior of the building as a whole.

ENCLOSURES:

1 PRELIMINARY PLAN SET for the REQUESTED PROPOSED ADDITIONS.

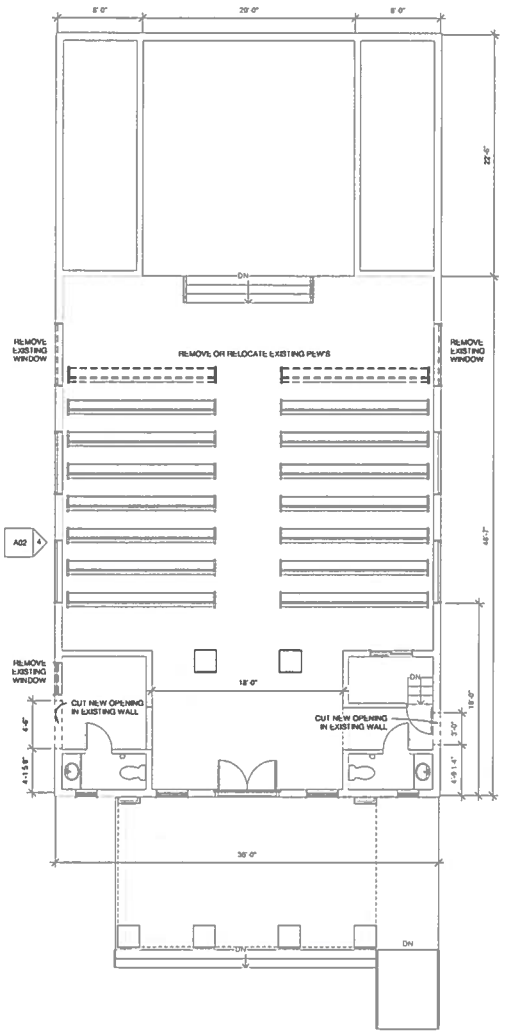
2 SITE PHOTOS

We do appreciate your time and consideration of what we would like to do in order to make "The Church at Koloa" a SAFE and PEACEFUL place to WORSHIP.
All are welcome to join us every Sunday at the 9AM service.

Respectfully submitted,

Nadine Begley

Nadine Begley
on behalf of: Pastor Harold Kilborn
Pastor Christy Kilborn
and the Board members of
"The Church at Koloa"



1 A01 EXISTING MAIN
3/16" = 1'-0"

2 A01 EXISTING FRONT VIEW

3 A01 PROPOSED FRONT VIEW

2 A02

4 A01 EXISTING 3D

5 A01 PROPOSED 3D

PRELIMINARY NOT FOR CONSTRUCTION

C&C
Chris St.Clair
4619 Lehua Street
Kapaa, Kauai, HI 96746
office: (808) 634-0471
e mail: 808cstc@gmail.com

SIGNATURE
"LICENSED 04/30/24"

THIS WORK WAS PREPARED BY ME OR UNDER MY SUPERVISION CONSTRUCTION OF THIS PROJECT WILL BE UNDER MY OBSERVATION. OBSERVATION OF CONSTRUCTION AS DEFINED IN CHAPTER 16 116 OF THE HAWAII ADMINISTRATIVE RULES DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS ENTITLED PROFESSIONAL ENGINEERS, ARCHITECTS, SURVEYORS AND LANDSCAPE ARCHITECTS

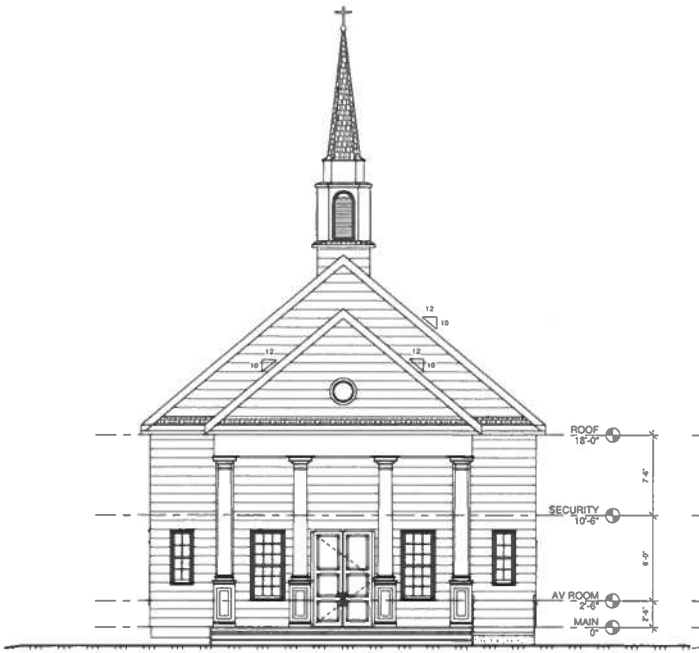
KOLOA HAWN PROTESTANT CHURCH
PROPOSED NEW STAIR, SECURITY ROOM AND FAMILY WASHROOM ADDITION
TMK (4) 2-8-010:008 & 009
KOLOA HAWAII 96756
2-8-010:008&009

EXISTING PLANS

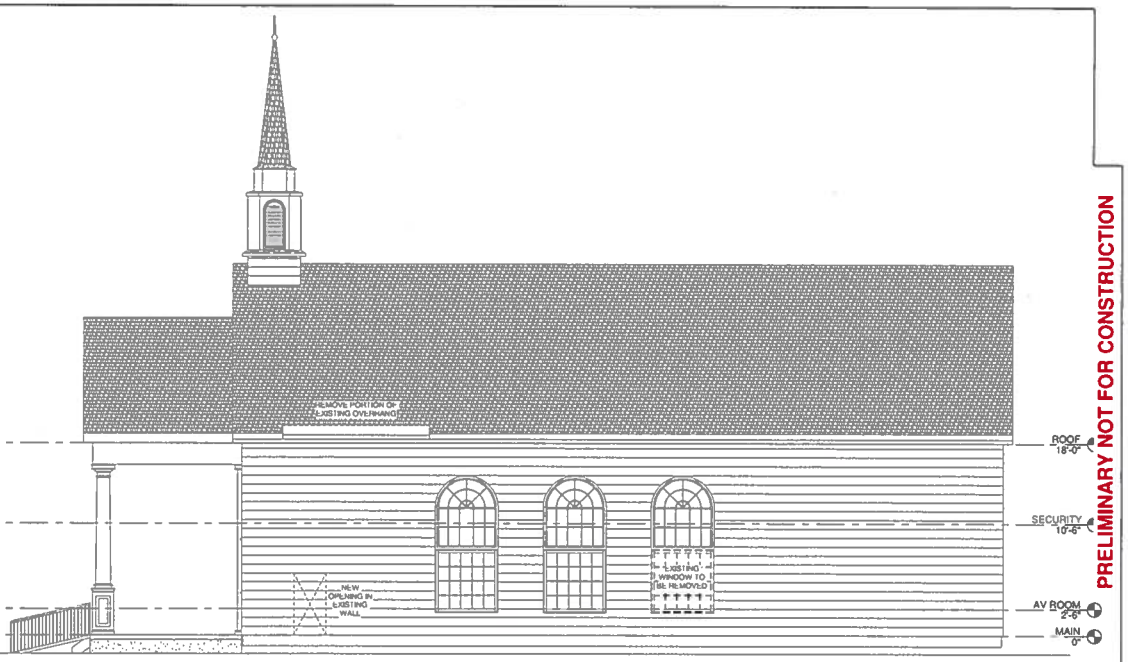
DATE
7/13/2023 1:00:16 PM

DRAWN BY
CSTC

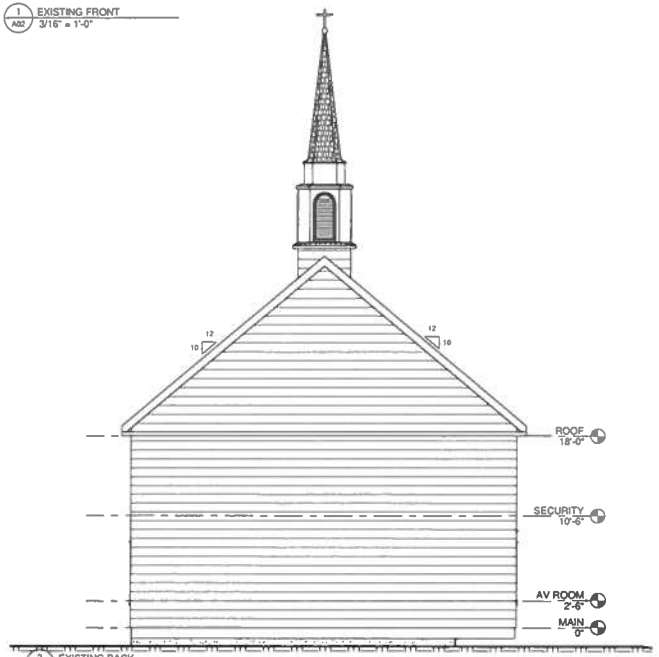
SHEET NO
A0 1



1 EXISTING FRONT
A02 3/16" = 1'-0"



2 EXISTING RIGHT
A02 3/16" = 1'-0"



3 EXISTING BACK
A02 3/16" = 1'-0"

4 EXISTING LEFT
A02 3/16" = 1'-0"

PRELIMINARY NOT FOR CONSTRUCTION

C&C
Chris St.Clair
4619 Lahua Street
Kapaa, Kauai, HI 96746
office: (808) 634-0471
e-mail: 808cscic@gmail.com

SIGNATURE
"LICENSED 04/30/24"

THIS WORK WAS PREPARED BY ME OR UNDER MY SUPERVISION. CONSTRUCTION OF THIS PROJECT WILL BE UNDER MY OBSERVATION. OBSERVATION OF CONSTRUCTION AS DEFINED IN CHAPTER 16 115 OF THE HAWAII ADMINISTRATIVE RULES, DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS ENTITLED PROFESSIONAL ENGINEERS, ARCHITECTS, SURVEYORS AND LANDSCAPE ARCHITECTS

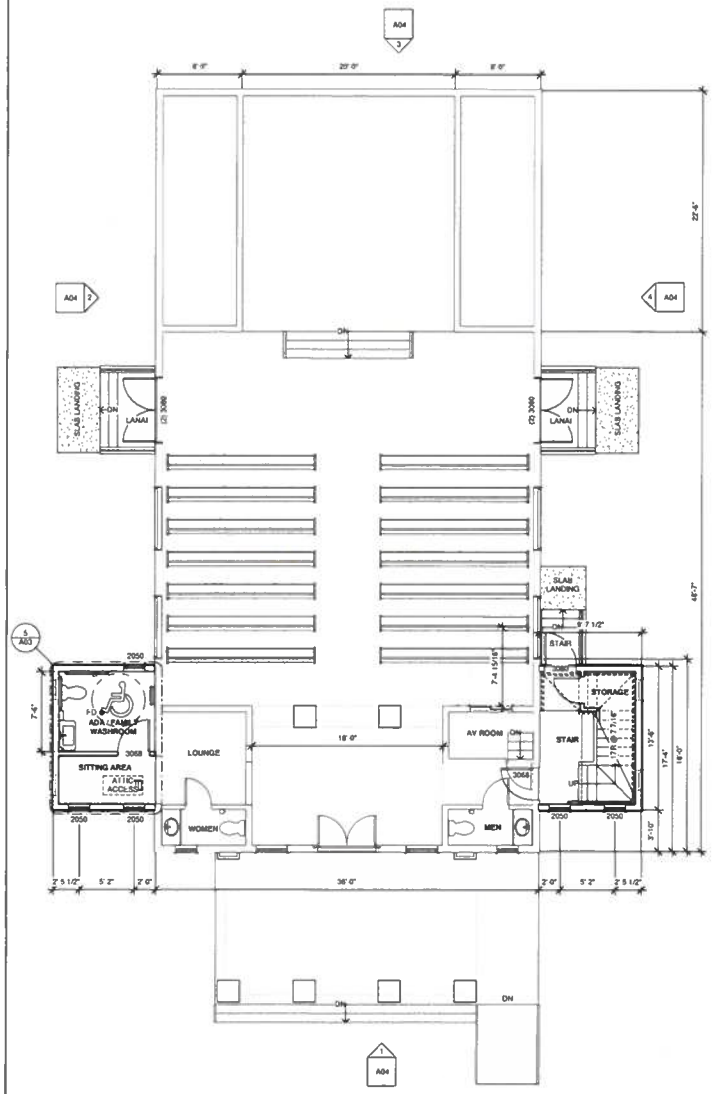
KOLOA HAWN PROTESTANT CHURCH
PROPOSED NEW STAIR, SECURITY ROOM AND FAMILY WASHROOM ADDITION
3281 POIPU RD
KOLOA, HAWAII 96756
2-6-010:008 & 009

EXISTING ELEVATIONS

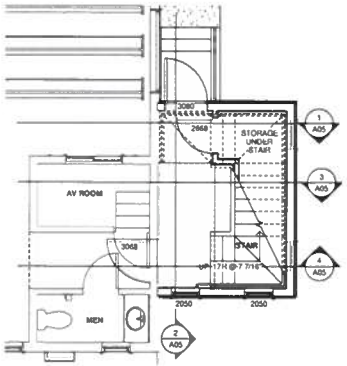
DATE
7/13/2023 1:00:17 PM

DRAWN BY
CSTC

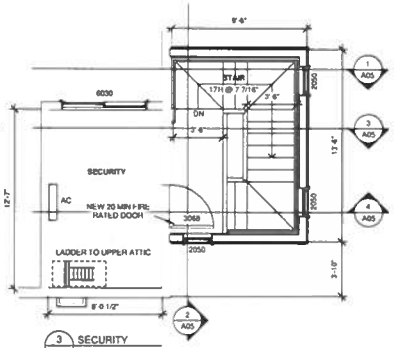
SHEET NO
A02



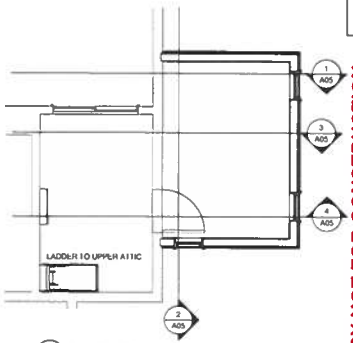
1 A03 PROPOSED MAIN 3/16" = 1'-0"



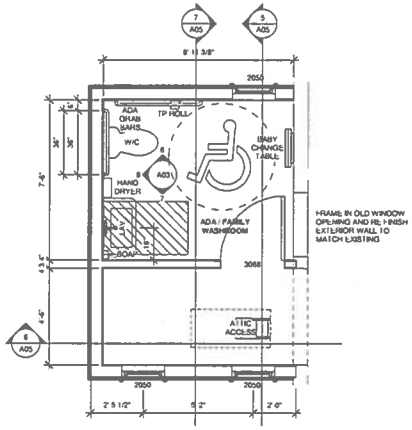
2 A03 MAIN STAIR 1/4" = 1'-0"



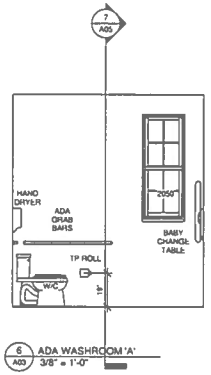
3 A03 SECURITY 1/4" = 1'-0"



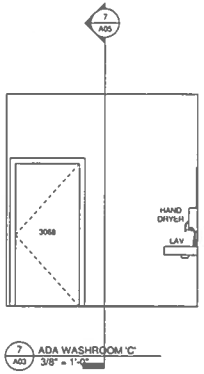
4 A03 SECURITY RCP 1/4" = 1'-0"



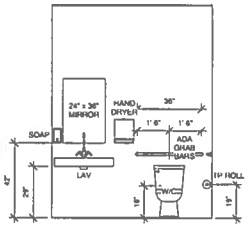
5 A03 ADA / FAMILY WASHROOM 3/8" = 1'-0"



6 A03 ADA WASHROOM 'A' 3/8" = 1'-0"



7 A03 ADA WASHROOM 'C' 3/8" = 1'-0"



8 A03 ADA WASHROOM 'D' 3/8" = 1'-0"

PRELIMINARY NOT FOR CONSTRUCTION

C&C
Chris St.Clair
4819 Lahua Street
Kapaa, Kauai, HI 96746
office (808) 634-0471
e-mail: 808cstc@gmail.com

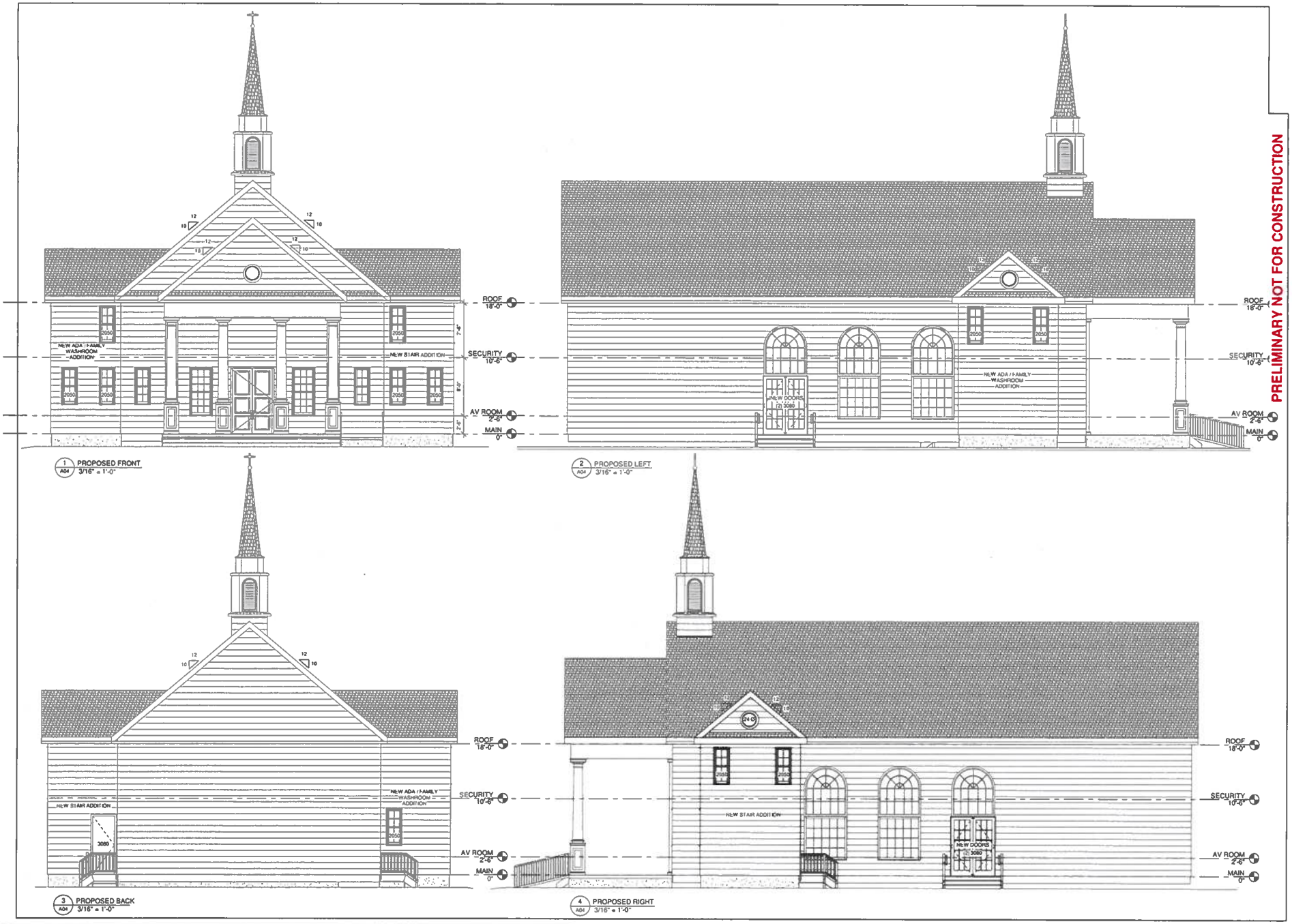
SIGNATURE
"LICENSED 04/30/24"

THIS WORK WAS PREPARED BY ME OR UNDER MY SUPERVISION CONSTRUCTION OF THIS PROJECT WILL BE UNDER MY OBSERVATION /OBSERVATION OF CONSTRUCTION AS DEFINED IN CHAPTER 16-115 OF THE HAWAII ADMINISTRATIVE RULES, DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS ENTITLED PROFESSIONAL ENGINEERS, ARCHITECTS, SURVEYORS AND LANDSCAPE ARCHITECTS)

KOLOA HAWN PROTESTANT CHURCH
PROPOSED NEW STAIR, SECURITY ROOM AND FAMILY WASHROOM ADDITION
3291 POIPU RD
KOLOA, HI 96756
2-8-010:008-0000

PROPOSED PLANS

DATE 7/13/2023 1:00:17 PM
DRAWN BY CSTC
SHEET NO. A03



1 A04 PROPOSED FRONT 3/16" = 1'-0"

2 A04 PROPOSED LEFT 3/16" = 1'-0"

3 A04 PROPOSED BACK 3/16" = 1'-0"

4 A04 PROPOSED RIGHT 3/16" = 1'-0"

PRELIMINARY NOT FOR CONSTRUCTION

Chris St.Clair
4619 Lehua Street
Kapaa, Kauai, HI 96746
office (808) 634-0471
e-mail: 808cstc@gmail.com

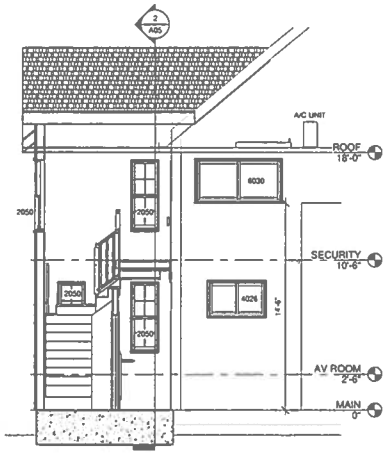
SIGNATURE
"EXPIRES 04/30/24"

THIS WORK WAS PREPARED BY ME OR UNDER MY SUPERVISION. CONSTRUCTION OF THIS PROJECT WILL BE UNDER MY OBSERVATION (OBSERVATION OF CONSTRUCTION AS DEFINED IN CHAPTER 16-115 OF THE HAWAII ADMINISTRATIVE RULES, DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS ENTITLED PROFESSIONAL ENGINEERS, ARCHITECTS, SURVEYORS AND LANDSCAPE ARCHITECTS)

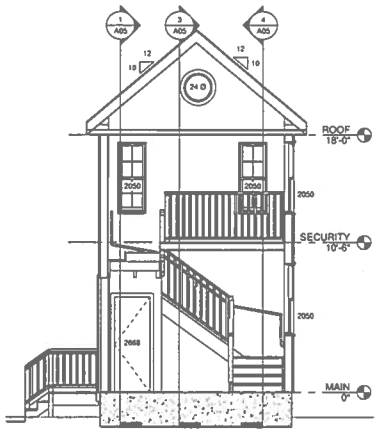
KOLOA HAWN PROTESTANT CHURCH
PROPOSED NEW STAIR, SECURITY ROOM AND FAMILY WASHROOM ADDITION
3251 POIPU RD
KOLOA HI 96756
2-8-010:006-0000

PROPOSED ELEVATIONS

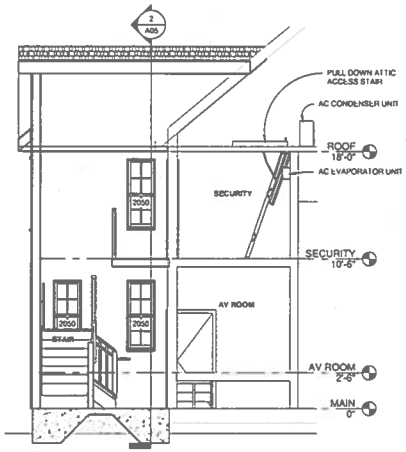
DATE 7/13/2023 1:00:18 PM
DRAWN BY CSTC
SHEET NO A04



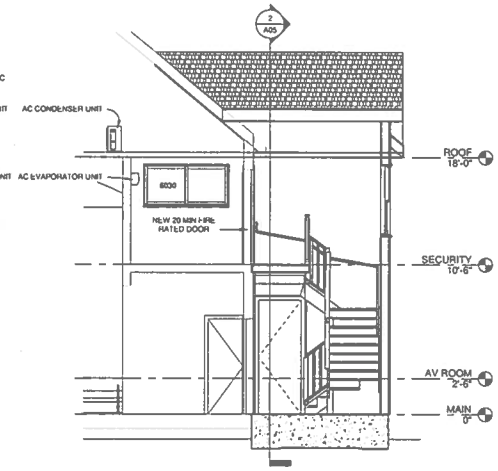
1 Section 1
A05 1/4" = 1'-0"



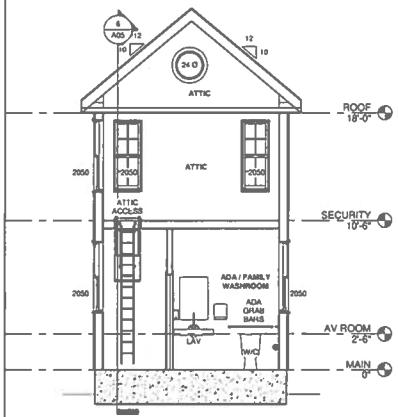
2 Section 2
A05 1/4" = 1'-0"



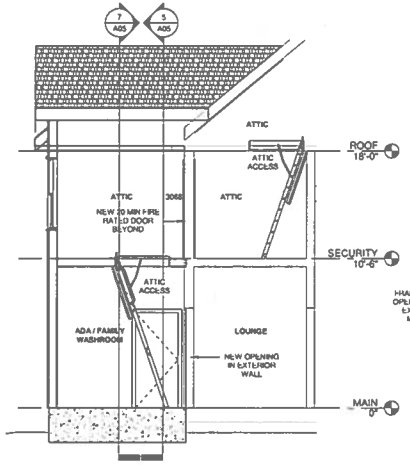
3 Section 3
A05 1/4" = 1'-0"



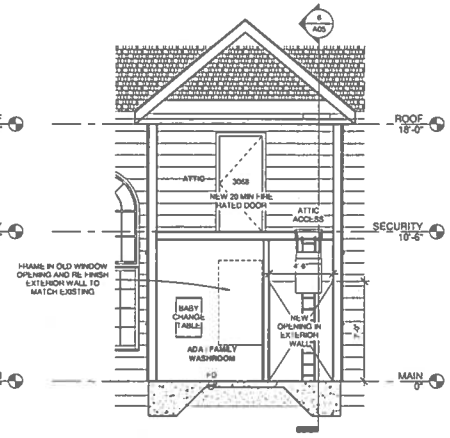
4 Section 4
A05 1/4" = 1'-0"



5 Section 5
A05 1/4" = 1'-0"



6 Section 6
A05 1/4" = 1'-0"



7 Section 7
A05 1/4" = 1'-0"

PRELIMINARY NOT FOR CONSTRUCTION

CSC
Chris St.Clair
4619 Lehua Street
Kapaa, Kauai, HI 96746
office (808) 634 0471
e mail 808cstc@gmail.com

SIGNATURE
"EXPIRES 04/30/24"

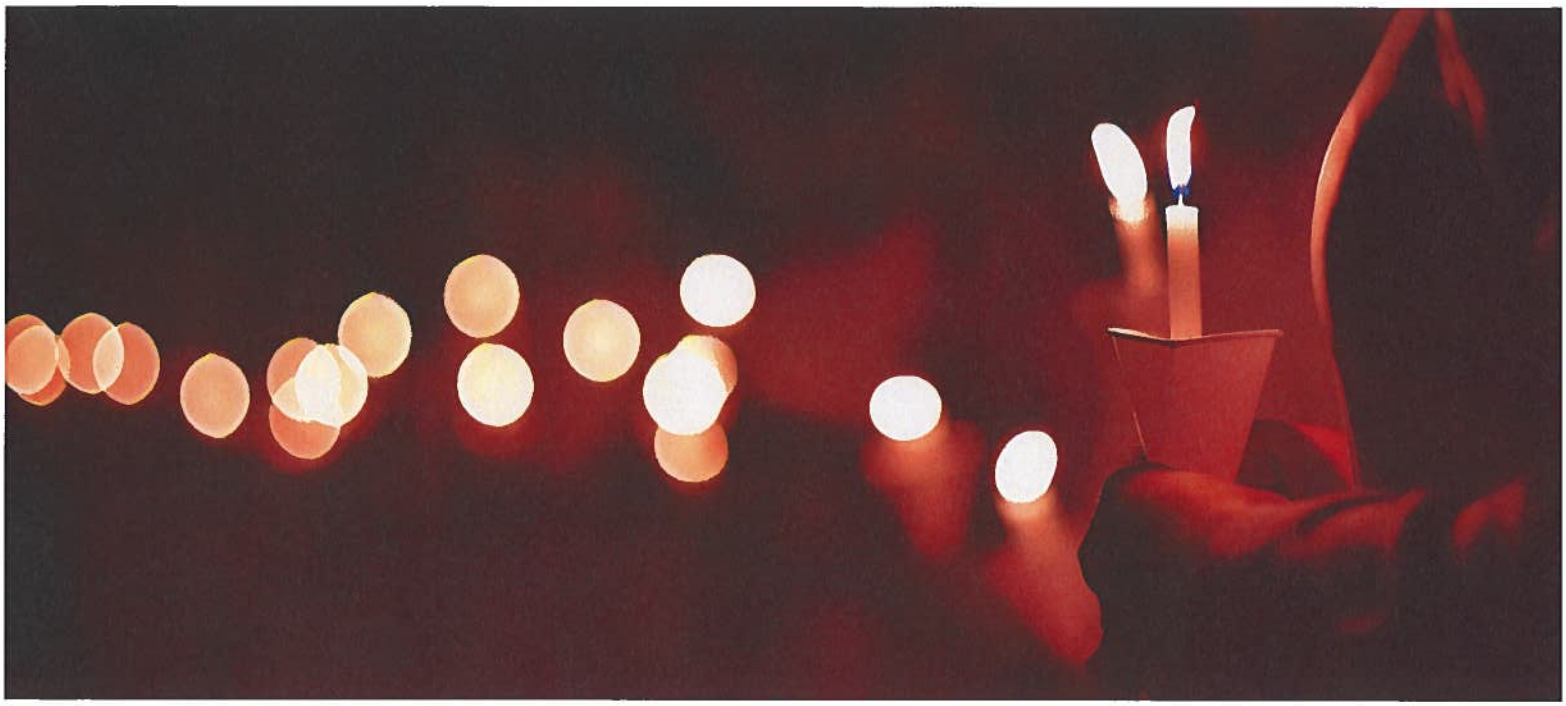
THIS WORK WAS PREPARED BY ME OR UNDER MY SUPERVISION. CONSTRUCTION OF THIS PROJECT WILL BE UNDER MY OBSERVATION. (OBSERVATION OF CONSTRUCTION AS DEFINED IN CHAPTER 16-115 OF THE HAWAII ADMINISTRATIVE RULES, DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS ENTITLED PROFESSIONAL ENGINEERS, ARCHITECTS, SURVEYORS AND LANDSCAPE ARCHITECTS)

KOLOA HAWN PROTESTANT CHURCH
PROPOSED NEW STAIR, SECURITY ROOM AND FAMILY WASHROOM ADDITION
3251 POPU RD
KOLOA HI 96756
2-8-010:008-0000

PROPOSED SECTIONS

DATE 7/13/2023 1:00:18 PM
DRAWN BY CSTC
SHEET NO A05

Exhibit A



MITIGATING ATTACKS ON HOUSES OF WORSHIP

Security Guide

DECEMBER 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

The best way to mitigate a potential attack is to take a holistic approach to security.

Contents

Letter from the Assistant Director 1

Executive Summary 2

Introduction: Protecting Houses of Worship 4

The Unique Role of Houses of Worship in American Society 4
Attacks on Houses of Worship 5
What is the Department of Homeland Security Doing? 5
What is CISA Doing? 6
Overview of the Guide 6

1 Understanding the Problem 9

Introduction 9
Review of Literature and National Trends 10
Methodology for Developing Case Studies 14

Targeted Violence 15
Operational Definition for Inclusion in Case Studies 15

Incident Case Studies 16

Overview of Incidents 16
Arsons and Bombings 17
Cyberattacks 20
Armed Assaults and Mass Shootings 20
Attack Outcomes 21
The Perpetrators 21
Targeted Houses of Worship 23

Perpetrator Tactics and Methods 24

Prior Association 24
Behavioral Indicators 24
Arsons & Bombings 24
Armed Assault 25
Cyber Attack 26

Security in Practice 28
Summary 28

2 Developing a Holistic Approach to Security 31

Introduction 31
What is a Holistic Approach to Security and How Do You Get There? 31
Key Concepts, Terms, and Questions 32
Framework for Developing a Holistic Security Strategy 35
Getting Started: Establishing Roles and Responsibilities 35
The Planning Process 36
Components of a Holistic Security Strategy: How to Secure Your House of Worship 36
Summary: Achieving a Holistic Security Strategy 37

3 Conducting a Comprehensive Vulnerability Assessment 39

Introduction 39
Assign Roles and Responsibilities 39
Determine the Scope of Your Vulnerability Assessment 40
A Vulnerability Assessment Model 41
Key Considerations for Leveraging the Vulnerability Assessment Model 42

Organizational Assets 42
Conduct As-Is Review 43
Comprehensive Threat Analysis 44
Identify Risk-Related Costs and Consequences 45
Determine Risk Solutions and Prioritize Mitigation 46

Summary 46

4 Building Community Readiness and Resilience 49

Introduction 49
Best Practices for Your HoW Community 49

Building a Culture of Safety 50
Awareness and Early Identification 50
If You See Something, Say Something® 51
Power of Hello 52
Run, Hide, Fight 53
Mental Health and Social Support Services 54

Specialized Policies and Long-Term Planning 55

Emergency Planning and Incident Response 55
Personnel Security Practices 56
Insider Threats 56
Reporting Procedures 57

Engaging the Wider Community 58

Event Planning 58
Community Engagement 59
Strategic Partnerships 60

Summary 61

5 Protecting Your Facilities 63
Introduction 63
Outer Perimeter 64
Middle Perimeter 66
Inner Perimeter 68
Summary 70

6 Daycare and School Safety Considerations 73
Introduction 73
Assess the Facilities 73
Procedures and Protocols 74
Physical Security 75
School Climate 75
Behavioral Health 76
Training 77
Funding Resources 78
Summary 78

7 Cybersecurity 81
Introduction 81
Types of Cyber Attacks 81
Financial Exploitation 81
Ransomware 82
Website Defacement 82
Creating a Culture of Cyber Readiness 82
Cyber Hygiene 83
Online Safety 84
Security Practices and Awareness 85
Combatting Specific Threats 87
Malware and Viruses 87
Phishing Attacks 87
Ransomware 88
Website Defacement 88
Summary 89

8 Summary and Overall Conclusions 90
Looking Forward 91

Appendix 1: Consolidated Resources for Houses of Worship 93

Chapter 1: Introduction 93
Chapter 2: Determining a Holistic Approach to Security 93

Emergency Preparedness 93
Emergency Operations 94
Business Continuity 94

Chapter 3: Conducting a Comprehensive Vulnerability Assessment 94
Chapter 4: Building Community Readiness and Resilience 95

Threat Management 95
Community Engagement and Community Relations 95
Professional Liaison Relationship 96
Mental Health and Social Support Services 96

Chapter 5: Protecting Your Facilities 96

Grants 96
Security Through Design 96
Threat Management 96

Chapter 6: Daycare and School Safety Considerations 97

General Resources 97
Physical Security 97
School Climate 97
Training 97
Funding Resources 98

Chapter 7: Cybersecurity 98

Cyber Hygiene 98
Online Safety 98
Security Practices and Awareness 99
Security Practices and Awareness (cont) 99
Malware and Viruses 99
Phishing Attacks 99
Ransomware 99
Website Defacement 99

Appendix 2: List of Incidents 101

List of Figures

Figure 1. FBI Hate Crime Data: incidents of religious bias and targeting of HoWs 13
Figure 2. FBI Hate Crime Data: individuals killed due to religious affiliation 14
Figure 3. Types of Attacks 17
Figure 4. Attacks by State 18
Figure 5. Incident Timeline 18
Figure 6. Active Shooter Timeline 20
Figure 7. Pre-Attack Planning Behaviors 21
Figure 8. Suspected Motive of Known Perpetrators 22
Figure 9. Reported Criminal History of Known Perpetrators 22
Figure 10. Denomination 23
Figure 11. Associations to Facility 23
Figure 12. The House of Worship Community 49
Figure 13. The "5Ws" of If You See Something, Say Something® 51

Security in Practice

Emergency Action Planning	28
Risk, Threat, Vulnerability, and consequence	32
CISA Protective Security Advisors	40
Pathway to Violence	50
Practicing the Power of Hello	52
Run, Hide, Fight	53
De-escalation	54
Professional Liaison Partnerships	60
Grant Funding	64
Security Through Design	64
Creating a Culture of Cyber Readiness	82
CISA Cybersecurity Advisors	83
Choosing Secure Passwords	84
Recognizing Phishing Attacks	87

A welcoming environment does not mean a defenseless one.

Letter from the Assistant Director

Freedom of religion is one of the fundamental liberties enshrined in the First Amendment of the United States Constitution. Yet recent attacks on worshipers of various faiths illustrate the unique safety challenges that face houses of worship across the country. Although the COVID-19 pandemic has temporarily limited our Nation's ability to come together in person, one day soon the American people will be able to safely gather in their faith communities and should do so without fear of harm.

The Cybersecurity and Infrastructure Security Agency (CISA) is committed to partnering with the faith-based community to help mitigate the threat of targeted violence and prepare for potential incidents.

Protecting houses of worship while preserving their welcoming and open environment is a priority for the agency. This guide presents new analysis drawn from a series of incidents over the past decade and offers a range of mitigation solutions designed to achieve a robust and layered approach to security.

As CISA's Acting Assistant Director for Infrastructure Security, I assure you that we continue to work diligently to identify innovative means through which we can collectively mitigate the risks we face as a Nation. Thank you for your commitment to securing our Nation and continued dedication to maintaining partnerships to protect the American people.

Sincerely,

Scott Breor
Acting Assistant Director for Infrastructure Security

Executive Summary

Acts of targeted violence against houses of worship (HoWs) are a real—and potentially growing—problem in the United States and a top priority for the U.S. Department of Homeland Security (DHS). As the Nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) prepared this guide to help faith-based organizations (FBOs) develop a comprehensive security strategy for adoption to the unique circumstances of every church, mosque, synagogue, temple, and other sites of religious practice across the country.

To better understand the nature of the problem, CISA drew on open source research to compile 37 incidents of targeted violence covering the ten-year period from 2009 to 2019. The analysis drawn from these case studies directly informs the guidance presented here and reveals several noteworthy trends.

- **CISA observed a significant spike in incidents of targeted violence in 2012 and a discernible increase in the number of incidents between 2015 and 2019. As a result of these 37 incidents, 64 people lost their lives and 59 people suffered injuries.**
- **Fifty-four percent** (n=20) **of the attacks were an armed assault of some kind, including shootings, edged weapons, and vehicular assaults. Five of the attacks qualified as mass shootings.**
- **CISA determined that 67 percent** (n=25) **of the attacks were motivated by hatred of a particular racial or religious identity, and that 22 percent** (n=8) **were connected to a domestic dispute or personal crisis. The motivation for the remaining 11 percent** (n=4) **is unknown.**
- **Of the 36 known perpetrators in these incidents, 58 percent** (n=21) **engaged in some form of planning behavior indicating their intention to carry out an attack.**

Within this analysis, CISA also describes several commonly used tactics and methods employed by the perpetrators. These tactics and methods point to specific areas of vulnerability that houses of worship can address through the security framework included within this guide. *The bottom line is that houses of worship can best protect themselves by adopting a comprehensive and multi-layered security strategy.*

To develop and implement a security program that can be adapted to the needs of individual houses of worship, CISA recommends the following overarching security actions:

- **Identify clear roles and responsibilities for developing and implementing security measures.**
- **Conduct a vulnerability assessment to understand the risks to your house of worship.**
- **Build community readiness and resilience by ensuring your house of worship is aware of potential threats, prepared to respond in the event of an emergency or incident, and connected with the wider community.**
- **Apply physical security measures to monitor and protect the outer, middle, and inner perimeters, while respecting the purpose of each area of the house of worship.**
- **Focus on the safety of children with security measures to protect childcare and daycare facilities and schools.**
- **Implement cybersecurity best practices to safeguard important information and prevent a potential cyberattack.**

These security options will not deter every threat to a house of worship, but a comprehensive security approach offers the best solution to protect people, property, and data. Houses of worship should tailor this knowledge to the needs of their communities while maintaining the open and welcoming atmosphere that makes houses of worship a critical part of the social fabric of the United States.

Introduction: Protecting Houses of Worship

The Unique Role of Houses of Worship in American Society

Religion is a powerful organizing force in communities across the country. According to the Pew Research Center's Religious Landscape Study, an estimated 36 percent of the American people attend religious services on a weekly basis. Factoring in those who attend on a monthly or yearly basis, the number grows to an estimated 69 percent. On important occasions, like weddings, funerals, and religious holidays, the number climbs even higher.[1]

Freedom of religion is a right guaranteed by the U.S. Constitution and recognized as a fundamental part of American society. Faith-based organizations (FBO) play a prominent role in providing social services such as food, shelter and clothing, and fostering a general sense of community. For many people, faith offers strength and hope; comfort and reassurance; moral compass and spiritual guidance; and triumph over stress and fear.

That sense of community and purpose is often physically centered around a house of worship (HoW). Churches, mosques, synagogues, temples, and other sites of religious practice are places of refuge and welcome, with few restrictions on access or admission. No matter their faith, houses of worship are nearly always designed to be open and accessible, reflecting a culture that is trusting and inviting.

A welcoming environment, however, does not mean a defenseless one.

Houses of worship face unique challenges as they strive for the right balance between security and accessibility. This guide offers context and guidance for HoWs to make informed decisions about the level of security that best fits their circumstances and environment.

---

1 "Attendance at religious services," Pew Research Center, https://www.pewforum.org/religious-landscape-study/attendance-at-religious-services/ (accessed July 9, 2020). See also "Fast Facts about American Religion," Hartford Institute for Religion Research, http://hartfordinstitute.org/research/fastfacts/fast_facts.html (accessed May 4, 2020)

Attacks on Houses of Worship

Over the last several years, attacks on houses of worship in cities like Charleston, Sutherland Springs, Pittsburgh, Poway, and Monsey have accelerated the national conversation around violence, social conflict, and mental health.

The analysis presented here by the Cybersecurity and Infrastructure Security Agency (CISA) indicates that such incidents of targeted violence have increased over the ten-year period from 2009 to 2019. The nature of these attacks varies widely, as do the denominations of the victims and the geographic regions in which the attacks took place.

CISA emphasizes, however, that such attacks remain statistically rare even as they appear to be on the rise. Each is a moment of profound trauma to those directly affected and to society at large. While these attacks have terrible impacts, it is important to maintain the social bond that make houses of worship a unique and integral part of the community. Houses of worship can accomplish many security measures without detracting from that special character. This guide intends to help houses of worship find the balance that fits best with their unique needs and circumstances.

What is the Department of Homeland Security Doing?

The Department of Homeland Security (DHS) identifies six overarching missions that comprise its strategic plan.[2] Three of those missions—countering terrorism and homeland security threats, securing cyberspace and critical infrastructure, and strengthening preparedness and resilience—directly touch our Nation's faith-based organizations and houses of worship as they endeavor to reduce the risk of violence and prevent attacks directed at their members and facilities.

In response to these recent attacks, DHS is increasing its efforts to strengthen prevention, preparedness, and mitigation resources for HoWs by providing information, training, exercises, and expertise. In April 2020, the Department designated the Office of Partnership and Engagement (OPE) to lead FBO security coordination. In June 2020, DHS also announced the creation of a Faith-Based Security Advisory Council (FBSAC) to provide recommendations on matters relating to houses of worship, faith-based organizations, and homeland security to the Secretary of Homeland Security.

This guide is part of CISA's ongoing effort to address this pressing security challenge. Given the nature of these attacks, this guide also represents part of the wider DHS effort to better understand and address acts of targeted violence.[3] Targeted violence and security for houses of worship are increasingly

2 "Strategic Planning," U.S. Department of Homeland Security, https://www.dhs.gov/strategic-planning

3 U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019, https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence

important missions across the Federal Government, as well as with state, local, tribal, and territorial governments (SLTT). This report builds on important work contributed by the U.S. Secret Service (USSS) National Threat Assessment Center (NTAC), the DHS Center for Faith and Opportunity Initiatives, and the U.S. Department of Justice (DOJ) Community Relations Service.

As with acts of terrorism, planning and target selection are hallmarks of targeted violence and offer critical opportunities for prevention, intervention, and risk mitigation. In this guide, CISA considers how some of the findings from previous work on targeted violence, such as school violence, can be applied to security planning for houses of worship.

What is CISA Doing?

The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA to lead federal cybersecurity and critical infrastructure security programs, operations, and policy.[4] As the Nation's risk advisor, CISA also has responsibilities for public gatherings, which are typically easily accessible and have limited security or protective measures in place.

Protecting public gatherings is one of CISA's most important missions and operational priorities.[5] Working in partnership with private entities, CISA provides leadership and support by identifying, developing, and implementing innovative and scalable measures to mitigate the risk to crowded places—including houses of worship.

Overview of the Guide

This guide offers new analysis, recommendations, and resources. Most importantly, this guide also presents a conceptual framework for both thinking about the security of HoWs and achieving a security plan best suited to the unique circumstances of every community.

CHAPTER 1 presents analysis based on ten years of incidents involving acts of targeted violence against houses of worship within the United States, including an overview of the tactics and methods most commonly used by perpetrators. The findings from this analysis directly inform the guidance offered in subsequent chapters.

CHAPTER 2 outlines a process for individual HoWs to think about their security needs and develop a robust and layered security strategy without sacrificing the unique qualities that make places of worship an important part of the local community.

---

4 Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115-278, U.S. Statues at Large 132 (2018): 4168-4186, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.

5 Cybersecurity and Infrastructure Security Agency, Strategic Intent, August 2019, https://www.cisa.gov/publication/strategic-intent. See also "Securing Soft Targets and Crowded Places," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securing-soft-targets-and-crowded-places.

CHAPTER 3 provides specific guidance on how to conduct a comprehensive *Vulnerability Assessment* that will help HoWs to evaluate their current security posture and specific needs.

CHAPTERS 4–7 offer more detailed discussions of the different aspects of security planning and the components that might be necessary for a HoW to achieve a layered security strategy.

Finally, **APPENDIX 1** presents a *Resource Guide* with a comprehensive list of the products that houses of worship can use to improve their overall safety and security. The chapter organizes resources by topic so that users can navigate the myriad of options and decision points that will be most beneficial for their needs.

Readers will also find these curated reference materials and resources throughout the guide. These resources—most of which have been produced by DHS and other security and law enforcement professionals—provide an opportunity for follow-up and further study for interested HoWs to continue their strategic security planning.

1 Understanding the Problem

Introduction

Houses of worship (HoWs) vary in size, denomination, and geographic location—and each has unique security needs. This guide is, in part, a direct response to a series of high-profile attacks that have captured national attention in recent years and troubled communities of all religious faiths. The guide also reflects general best practices for protecting crowds, tempered by the special considerations that come with HoWs.

To better understand how the problem of violence against sites of religious practice has evolved in recent years and address the wide range of security needs that exist across the Nation, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a thorough review of the literature and scholarship on the subject and examined ten years of data from open-source research, media reports, and national databases to compile a list of 37 case study incidents from 2009 to 2019. Together with the existing literature, these case studies reveal high-level trends and important lessons on the steps that can be taken to make houses of worship more secure.

These lessons directly inform the security options outlined in this guide. In sum, the research makes clear that HoWs face a variety of security challenges and point to the need for a comprehensive and multi-layered approach to security.

Review of Literature and National Trends

Scholars estimate there are approximately 350,000 to 400,000 individual congregations within the United States.[1] Each represents a critical part of the local community, and houses of worship of all faiths are traditionally regarded as sanctuaries that value openness and inclusion. At the same time, that openness, social prominence, and symbolic importance create unique security challenges.

CISA reviewed literature from a wide range of fields and disciplines for this guide, including: open source media reports; scholarly publications in peer-reviewed journals; government reports, documents, and databases; and articles published by law enforcement, threat assessments, and other security professionals.

Houses of worship vary in size, denomination, and geographic location ...

Overall, the field of HoW security is relatively small and there is even less established literature on the specific problem of targeted violence. Security professionals have increased their attention to the needs of churches, synagogues, mosques, temples, and other religious sites in recent years, but most of the literature produced by industry is proscriptive (rather than analytical) in nature.[2] Scholars, meanwhile, have just begun to conduct systematic research on acts of violence targeting HoWs.[3] Just as researchers cannot state with any certainty the precise number of individual congregations within the United States, there is no precise accounting for the number of violent acts deliberately targeting houses of worship.

One challenge is the need for a unified and robust tracking system. Existing research and analysis often come from media reports or unconnected databases such as *The Violence Project* at Hamline University[4] or the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program, which aggregates hate crimes reported by local jurisdictions.[5] Most researchers contend that such databases, while useful, are limited by incomplete or

1 C. Kirk Hadaway and Penny Long Marler, "How Many Americans Attend Worship Each Week? An Alternative Approach to Measurement," *Journal for the Scientific Study of Religion* (2005), 44 (3): 307-322; Simon Brauer, "How Many Congregations Are There? Updating a Survey-Based Estimate," *Journal for the Scientific Study of Religion* (2017) 56 (2): 438-448

2 Jim McGuffey, Paula L. Ratliff, Doug Meacham, Phil Purpura, Dick Raisler, Carl Chinn, and Alistair Calton, *Securing HoWs Around the World* (ASIS International, 2017), https://www.asisonline.org/globalassets/get-involved/councils/documents/best-practices-securing-houses-of-worship.pdf

3 For a brief description of the existing scholarly literature, see Christopher P. Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports," *International Review of Victimology* 22 (1), January 2016: 65-74 and Christopher P. Scheitle and Caitlin Halligan, "Explaining the adoption of security measures by places of worship: perceived risk of victimization and organizational structure," *Security Journal* 31, July 2018: 685-707.

4 "The Mass Shooter Database," *The Violence Project*, https://www.theviolenceproject.org/

5 "Uniform Crime Reporting Program," Federal Bureau of Investigation, https://www.fbi.gov/services/cjis/ucr/

inconsistent reporting and hypothesize that the incidents recorded therein likely represent an undercount.[6]

Even so, the data points to two distinct trends: that HoWs face a baseline of persistent targeted criminal activity and that the specific threat of targeted violence may be increasing.

On one end of the spectrum are the type of incidents that are statistically common but not necessarily life threatening. Vandalism, for example, appears to be a routine problem for HoWs across the country.[7] Yet HoWs also appear to face a certain level of persistent life-threatening violence, but which may fall short of the criteria for targeted violence used in this guide. One estimate based on FBI data projects that between 2000 and 2016 there were approximately 480 violent incidents per year—including armed robberies, assaults, and bombings—resulting in 46 deaths and 218 serious injuries annually.[8]

... and each has unique security needs.

On the other end of the spectrum is the growing problem of mass shootings, which are statistically rare but represent the greatest trauma and loss of life. Such attacks have increased in the last five years alongside the general upward trend in mass shootings nationwide and often meet the definition of targeted violence (outlined below). The attack on the Baptist church in Sutherland Springs, for example, was the fifth deadliest mass shooting incident in the United States tracked by the *Violence Project*.[9]

Qualitatively, a strong association appears to exist between social climate and threats to HoWs. Historical analysis reveals that attacks on distinct ethnic and religious groups and individual houses of worship often accompany periods of intense racial and religious strife. Some well-known examples include the bombing and burning of black churches or the defacement and vandalism of synagogues and mosques during outbursts of anti-Semitism and anti-Muslim animus.[10]

6 Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports."

7 Christopher P. Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports," *International Review of Victimology* 22 (1), January 2016: 65-74; William Bourns and Wesley D. Wright. "A Study of Church Vulnerability to Violence: Implications for Law Enforcement," *Journal of Criminal Justice* 32 (2), March 2004: 151–157

8 "Serious violence at places of worship in the U.S.—Looking at the numbers," Dolan Consulting Group, September 9, 2019, https://www.dolanconsultinggroup.com/news/serious-violence-at-places-of-worship-in-the-u-s-looking-at-the-numbers/

9 Jillian Peterson and James Densely, "Opinion: Why do people attacks places of worship? Here's what we know from our mass shootings database," *Los Angeles Times*, December 30, 2019; Jilian K. Peterson and James A. Densely, "The Violence Project: Database of Mass Shootings in the United States, 1966-2019," November 2019, p. 16, https://www.theviolenceproject.org/

10 For a selection of more recent examples, see: John P Bartkowski, Frank M Howell, and Lai Shu-Chuan, "Spatial variations in church burnings: The social ecology of victimized communities in the South," *Rural Sociology* 67 (4), December 2002: 578–602; Yehudut Barsky, "Terrorist Incidents and Attacks Against Jews and Israelis in the United States," Community Security Service, 2016, https://jewishpgh.org/app/uploads/2018/09/Terrorist-Attacks-Against-Jews-in-US-1969-2016.pdf; American Civil Liberties Union,

Troubling signs indicate that the country has once again entered a period of social unrest with a simultaneous rise in bias-motivated attacks and hate crimes. The *Associated Press* points out that three of the deadliest attacks on HoWs have occurred since 2015. The rise of social media, meanwhile, has created fertile ground for hate speech and hateful ideologies to flourish within certain corners of the internet.[11]

To meet these challenges, the Department of Homeland Security (DHS) has directed a growing number of resources to address the specific problem of targeted violence and in September 2019 published *Strategic Framework for Countering Terrorism and Targeted Violence* to better coordinate government action. The report is noteworthy for calling new attention to security threats originating within the United States. DHS identified two broad categories of special concern: (1) homegrown violent extremists (HVEs) motivated by the messaging and ideologies of foreign terrorist organizations and (2) domestic terrorists, particularly with those associated with white supremacist violent extremism.[12] Both categories represent a potential threat to HoWs.

In addition, the COVID-19 pandemic may be increasing the prevalence of hate crimes and racial prejudice across the western world, further exacerbating the threat to HoWs and prompting CISA to issue an advisory to religious organizations, cautioning that "stressors caused by the pandemic may contribute to an individual's decision to commit an attack or influence their target of choice."[13]

Alongside the more random and unpredictable attacks driven by personal and domestic crisis, the growing prevalence of hate-motivated attacks, portrayed in Figures 1 (p. 13) and 2 (p. 14), represents a grave risk to HoWs within the United States.

"Nationwide Anti-Mosque Activity," December 2019, https://www.aclu.org/issues/national-security/discriminatory-profiling/nationwide-anti-mosque-activity.

11 Adeel Hassan, "Hate-Crime Violence Hits 16-Year High, FBI Reports," New York Times, November 12, 2019; Federal Bureau of Investigation, "2018 Hate Crime Statistics," https://ucr.fbi.gov/hate-crime/2018/hate-crime; Gary Fields and David Crary, "Year-end violence highlights danger of worshipping," *Associated Press*, January 1, 2020; Marc Fisher, Roxana Popescu, and Kayla Epstein, "Ancient hatreds, modern methods: How social media and political division feed attacks on sacred spaces," Washington Post, April 28, 2019.

12 U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019, https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence.

13 Anna Russel, "The rise of coronavirus hate crimes," New Yorker, March 17, 2020; Natasha Bertrand, "DHS warns pandemic 'stressors' could trigger attacks on HoWs," *Politico*, April 8, 2020.

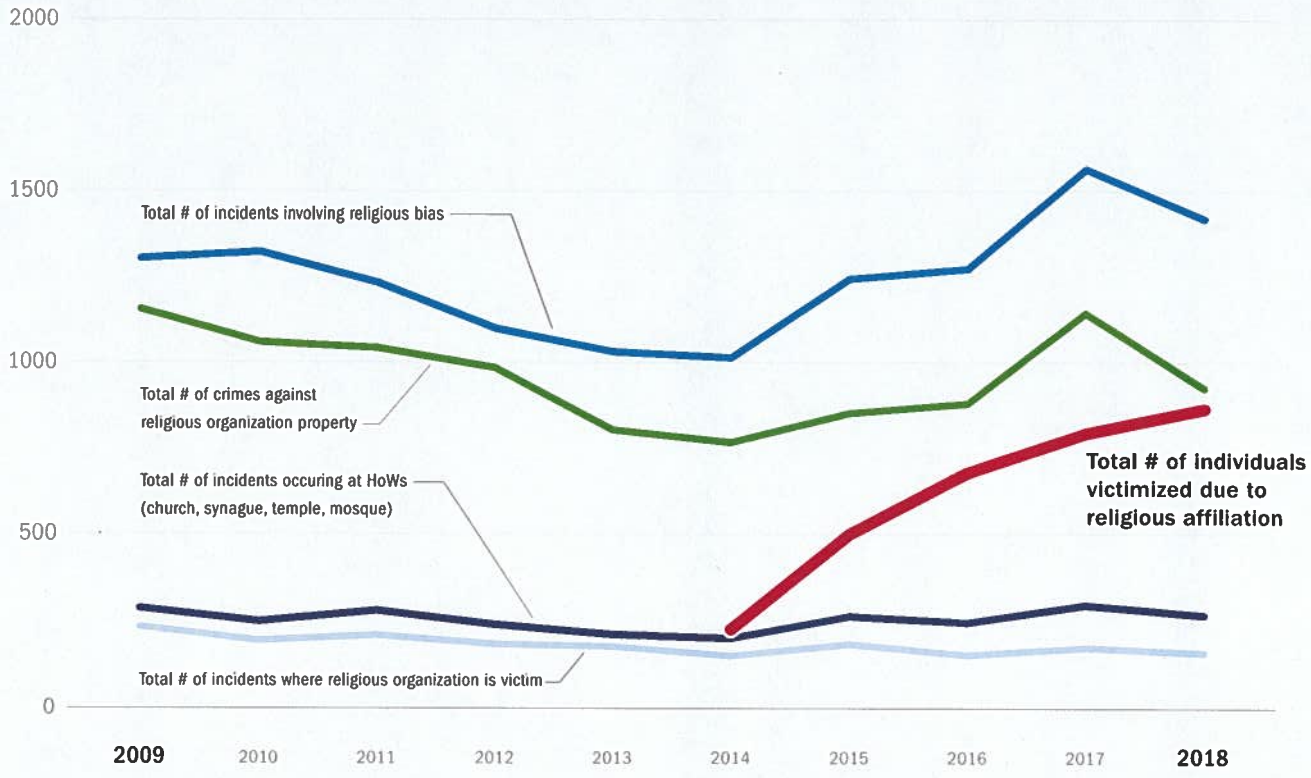


Figure 1. FBI Hate Crime Data: incidents of religious bias and targeting of HoWs

Figure 1 displays a series of categories compiled in the FBI Hate Crime Data as they relate to religious bias. The medium blue line (top) tracks the total number of hate crime incidents involving religious bias. The green line tracks the number of property crimes committed against religious organizations. The red line tracks the number of individuals victimized (including murder/manslaughter, rape, aggravated assault, simple assault, intimidation, and other) for reasons of religious affiliation, a distinct category the FBI began keeping in 2014. The light blue line (bottom) tracks the number of incidents in which a religious organization is recorded as the victim. The dark blue line (second from bottom) tracks the total number of hate crime incidents occurring at HoWs. Data for 2019 was not available at the time of publication.

Together, these data trends provide valuable insight into the overall tone of American civic life and prevalence of hate crimes involving religion.

Source: FBI UCR hate crime statistics, tables 1, 7, 8, and 10 https://www.fbi.gov/services/cjis/ucr/hate-crime

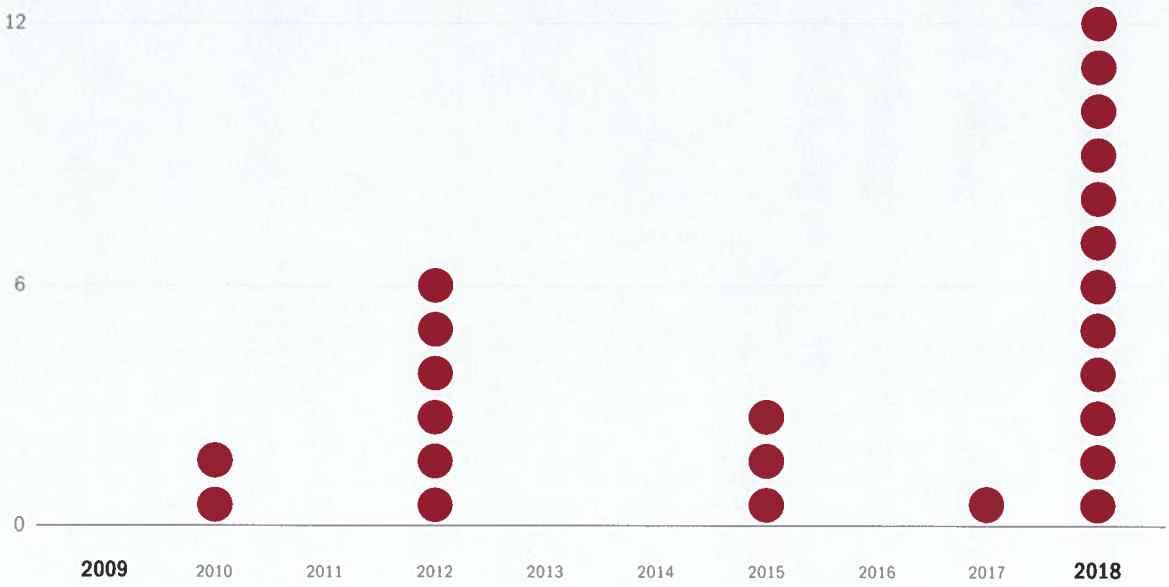


Figure 2. FBI Hate Crime Data: individuals killed due to religious affiliation

Figure 2 shows the number of individuals killed due to reasons of religious affiliation and bias as tracked by FBI Hate Crime statistics. This number is included as a subset of the total number of individuals victimized for religious affiliation reflected in figure 1.

Source: FBI UCR hate crime statistics, table 7, https://www.fbi.gov/services/cjis/ucr/hate-crime

Methodology for Developing Case Studies

To supplement existing research and provide context for the security considerations included within this guide, CISA developed a series of case studies to track targeted violence against HoWs during the ten-year period between 2009 and 2019. CISA gathered these incidents through a thorough search of a variety of sources, including: FBI Hate Crime Statistics (part of the UCR Program); the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Bomb Arson Tracking System (BATS); DHS's Technical Resource for Incident Prevention (TRIP*wire*); the University of Maryland's Global Terrorism Database; and Hamline University's *The Violence Project*. However, CISA drew most of the case studies from open-source media reports, which provided the most substantive publicly available information. Although some details were limited or incomplete, CISA corroborated the essential facts with multiple sources whenever possible.

To separate acts of deliberate violence from random acts of crime, CISA used the following definition as criteria for inclusion within these case studies: *An act of targeted violence against a house of worship or affiliated property within the United States that results in significant damage, injury, or loss of life.*

The number of cases that met the criteria for inclusion was relatively small—compared, for example, to the data offered in FBI Hate Crime Statistics—and CISA anticipates there are additional incidents that have not been included or evaluated in this guide.

Targeted Violence

Targeted violence refers to violence that is goal-directed and focused on specific individuals, groups, or locations. Perpetrators select their targets to achieve specific motives, such as the resolution of a grievance or to make a political or ideological statement. Targeted violence is distinct from violence that is impulsive, random, or spontaneous and often distinguished by clear indicators or pre-attack planning behaviors. Those behaviors, if detected, can be useful to thwart or mitigate an incident.

The 2019 DHS Strategic Framework defines targeted violence as:

> . . . any incident of violence that implicates homeland security and/or DHS activities, and in which a known or knowable attacker selects a particular target prior to the violent attack. Unlike terrorism, targeted violence includes attacks otherwise lacking a clearly discernible political, ideological, or religious motivation, but that are of such severity and magnitude as to suggest an intent to inflict a degree of mass injury, destruction, or death commensurate with known terrorist tactics.[14]

Operational Definition for Inclusion in Case Studies

For the purpose of this analysis, CISA focused on incidents within the United States during the period from 2009 to 2019 and defined "an act of targeted violence against a HoW" as any incident in which a perpetrator deliberately targeted a HoW to:

1. Kill or injure one or more persons affiliated with a HoW, including clergy, staff, and congregants;
2. Cause significant property damage to a HoW; and/or
3. Engage in cybercrimes targeting a HoW, including such acts as network intrusions, software piracy, identity theft, financial fraud, and phishing.

---

14 U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019, p. 4. See also Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *Research in Action* (National Institute of Justice, U.S. Department of Justice), July 1995.

This analysis is limited to incidents of targeted violence and does **NOT** include:

- **Incidents where a perpetrator could not be identified or a focused interest in the HoW could not be determined;**
- **Incidents resulting in minor property damage;**
- **Incidents of minor assault, burglary, graffiti, theft, etc.;**
- **Incidents related to gang violence, drug violence, or other incidents with a separate criminal nexus;**
- **Violence from the surrounding community that encroached onto HoW property by happenstance;**
- **Spontaneous, impulsive acts that were not planned and where the HoW was not specifically targeted.**

Incident Case Studies

A detailed search produced a total of 37 separate incidents that met the operational definition. Although a truly comprehensive understanding of national trends requires more data, these case studies offer a start and an approximation of how targeted violence against HoWs has evolved over the last decade. More importantly, in-depth study of these case studies yields important insights into the tactics and methods used by the attackers. Properly applied, those insights can help to anticipate vulnerabilities and mitigate threats.

For a full list of incidents, see APPENDIX 2.

Overview of Incidents

Overall, CISA found targeted violence against houses of worship to have religious, racial, and personal ideological motivations and to affect HoWs of all sizes and denominations. The incidents reviewed here occurred in 20 states across the Nation and included both urban and rural locations, as indicated in Figure 4 (p. 18–19).

Though not determinative, a timeline of the case studies (Figure 5, p. 18) confirms media accounts depicting an increase in incidents of violence against HoWs over the 10-year period from 2009 to 2019. This timeline reveals that while the number of incidents of this magnitude has not increased each year, there was a notable increase in the number of attacks between 2015 and 2019, indicating that violence targeting houses of worship remains a genuine threat to the American people.

Types of Attacks

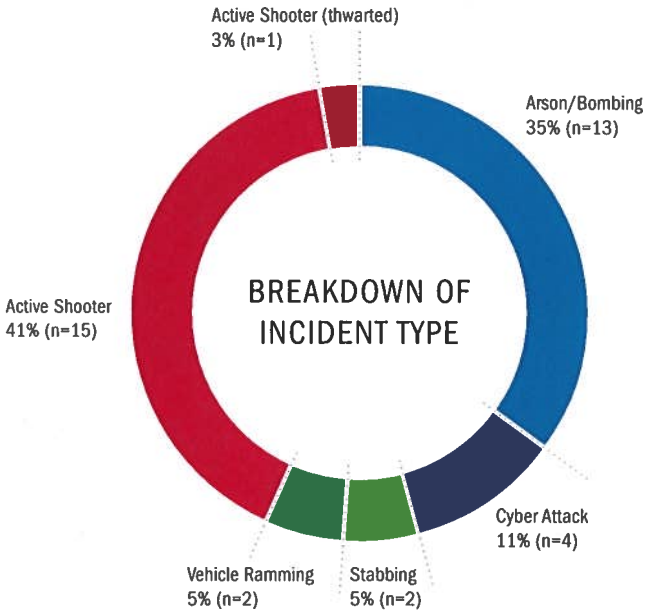
CISA examined a range of incidents, including active shootings, stabbings, cyberattacks, arsons, bombings, and vehicle rammings, shown in Figure 3. Over half (54 percent, n=20) of the case studies identified represent an armed assault of some kind, including shootings, edged attacks, and vehicular attacks. Included in this study is one incident of a thwarted active shooter scenario as an important training tool in de-escalation strategies for all HoWs to consider.

The assailants relied on a range of weapons—from guns and knives to explosives or incendiary devices and network exploitation tools—to carry out their attacks. Guns were the most common weapon (n=16), followed by incendiary devices (n=6) and cyberattacks (n=4).

Figures 4 and 5 (p. 18–19) depict the attacks by location and the year each incident occurred.

Figure 3. Types of Attacks

Figure 3 shows the breakdown in type of attacks that fit CISA's criteria for an act of targeted violence against a house of worship.



Arsons and Bombings

CISA identified 13 incidents of arson or bombing. Although each represents a distinct category of attack, arsons and bombings are often tracked together by federal agencies such as the ATF and CISA's Office for Bombing Prevention (OBP). The analysis of these 13 incidents revealed a mix of devices, including the use of gasoline accelerants (n=4), improvised incendiary devices (IIDs) such as Molotov cocktails (n=6), and improvised explosive devices (IEDs) such as pipe bombs (n=1). One of the attacks included both an IID and IED. In three of the attacks, each of which was an arson, the type of accelerant or flammable material used was not reported. CISA found that 85 percent (n=11) of these attacks were motivated by hatred of a particular religious or racial identity.

These 13 incidents are indicative of a much larger phenomenon. Most arson cases target buildings after normal business hours and are usually intended to inflict property damage. On the other hand, in bombing cases, perpetrators typically intend to harm individuals gathered at a specific location. Historically, both arsons and bombings have long been used to target houses of worship in the United States, and bomb threats often serve as a tool of intimidation. CISA anticipates there may well be additional cases of arsons and bombings that targeted HoWs during this ten-year period but were not included in this analysis.

ARSON AND BOMBING TYPES:

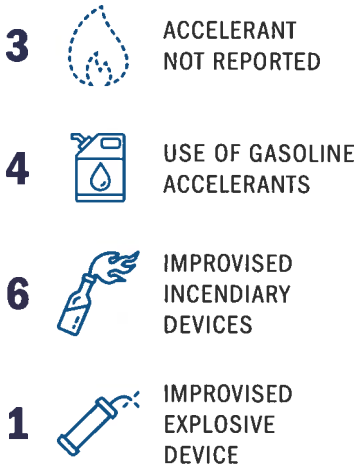
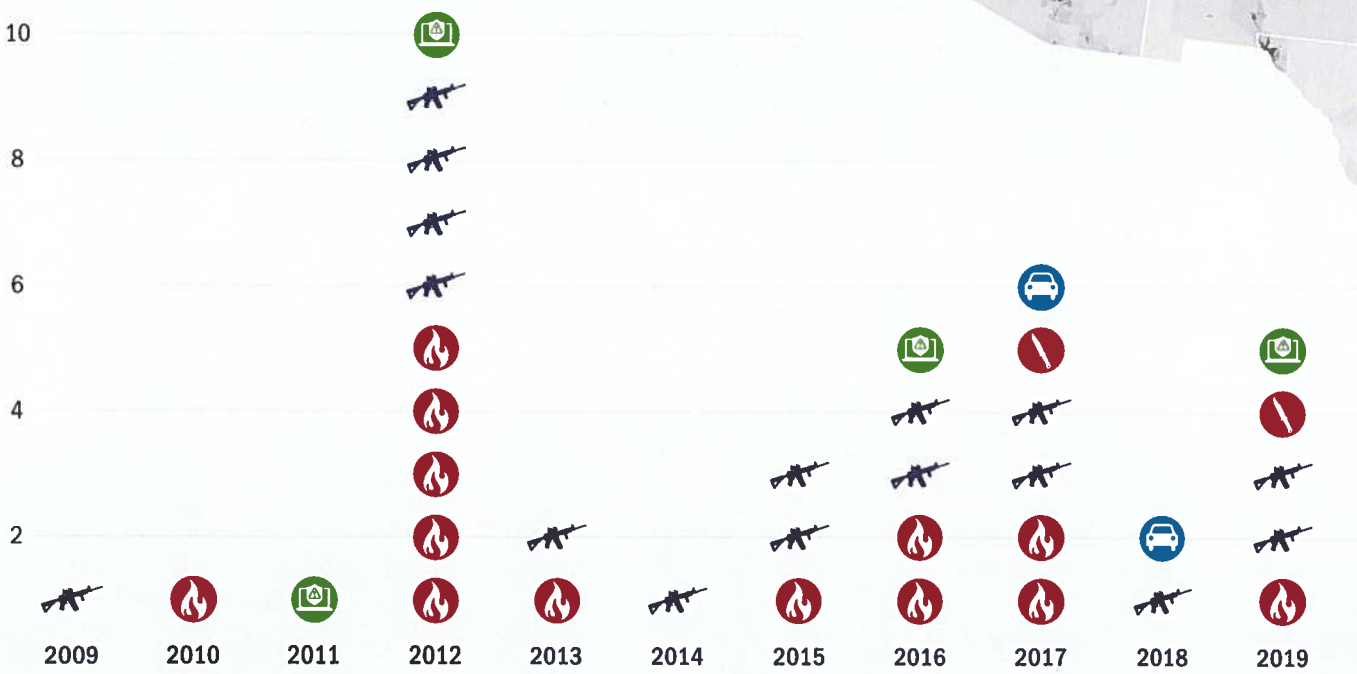


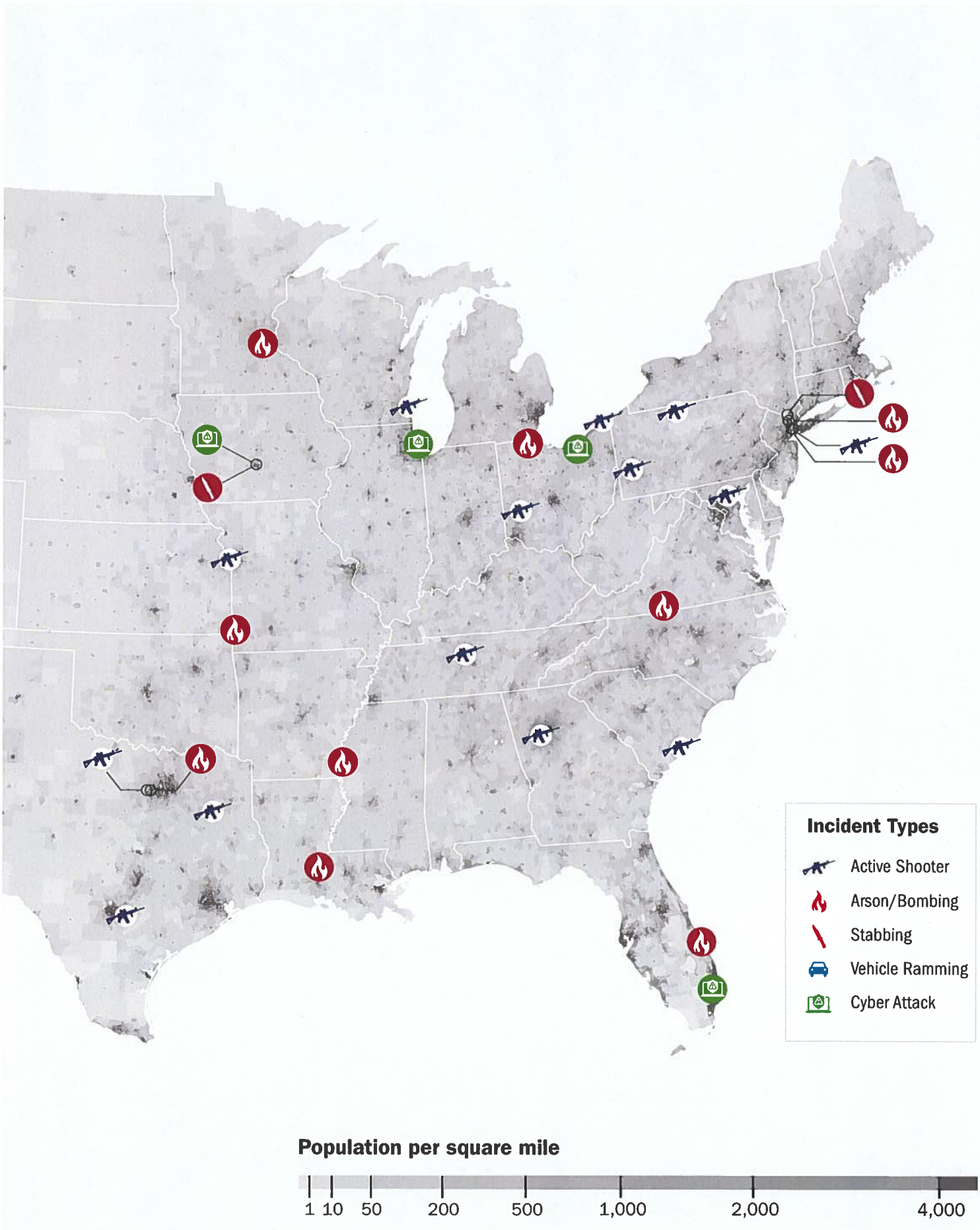
Figure 4. Attacks by State

Figure 4 identifies the attacks (n=37) by state. The incidents reviewed here occurred in 20 states across the Nation and included both urban and rural locations.

Figure 5. Incident Timeline

Figure 5 illustrates the timeline of the incidents (n=37) across the period of study.




Incident Types
Active Shooter
Arson/Bombing
Stabbing
Vehicle Ramming
Cyber Attack
Population per square mile
1
10
50
200
500
1,000
2,000
4,000

Cyberattacks

CISA reviewed four cyberattacks on HoWs, including two incidents of financial schemes and two incidents of website defacement. Financial damages to the HoWs were $680,000 and $1,750,000 respectively, as well as the worry and damage to reputation that resulted from website defacement. As with most cybercrimes, the attacks had no known perpetrator. Whether the website defacements and financial hacks were ideologically motivated or crimes of opportunity is unclear.

Armed Assaults and Mass Shootings

Of the cases examined, 54 percent (n=20) qualified as an armed assault of some kind, be it with a gun, knife, or vehicle that was deliberately used to harm individuals at a HoW. Mass shootings are included in the armed assault data and represent the incidents with the greatest loss of life. Definitions of mass shooting vary, but typically entail the use of a firearm to kill or injure four or more individuals at the same time and place. Fifteen active shooter events and five mass shootings are included in this report.

The mass shootings identified for this report included several common tactics and methods and informed many of our recommendations. See Figure 6 for a timeline of these incidents.

MASS SHOOTING EVENTS:

In August 2012, a 40-year-old man armed with a handgun began shooting outside the Sikh Temple of Wisconsin in Oak Creek, Wisconsin and then moved inside and continued to shoot congregation members. Police confronted the shooter as he exited the building. Six people lost their lives, and four people, including one police officer, suffered injuries. The shooter committed suicide after he was shot in the stomach by responding officers.

In April 2014, a 73-year-old man armed with two handguns and a shotgun began shooting in the parking lot of the Jewish Community Center of Greater Kansas City in Overland Park, Kansas, killing two. He then drove to the nearby Village Shalom retirement community and opened fire in the parking lot, killing one. No one else was wounded. Law enforcement apprehended the shooter who later received the death sentence.

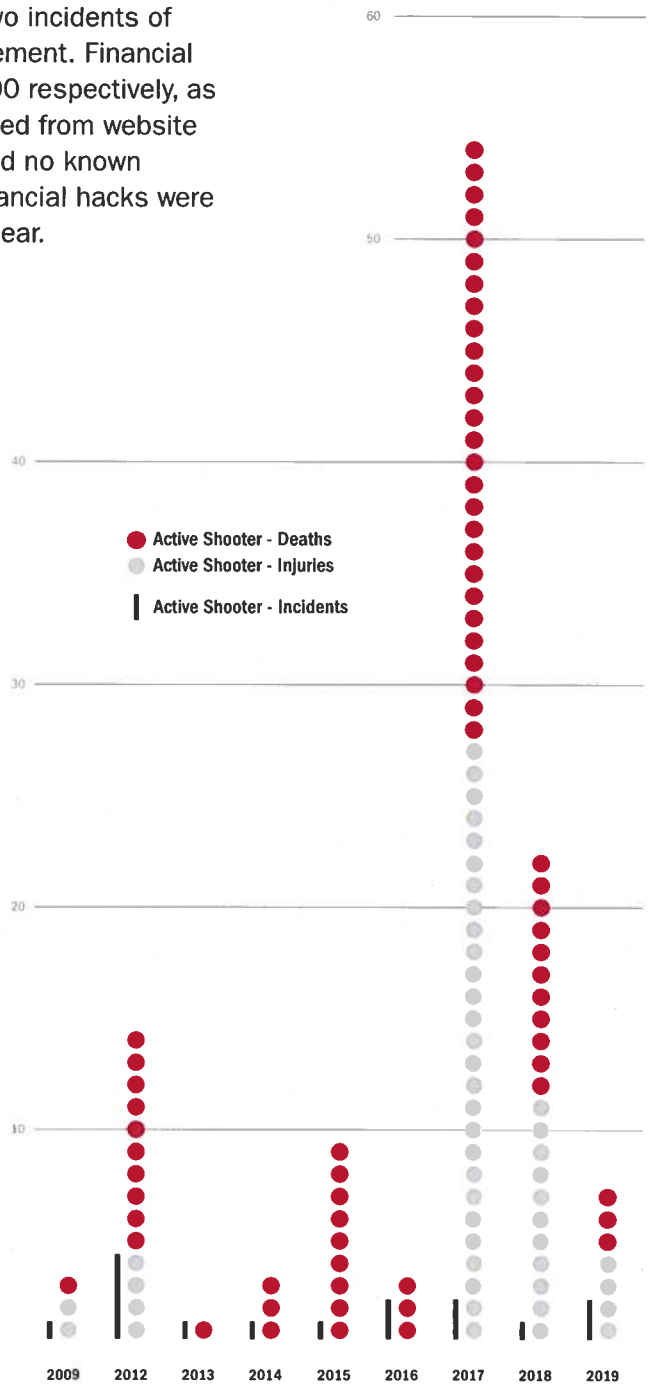


Figure 6. Active Shooter Timeline

Figure 6 illustrates the timeline for active shooter incidents included in the analysis (n=15 Active Shootings). The significant spike in deaths and injuries in 2017 was due to the mass shooting at Sutherland Springs, Texas, in which 26 people were killed and 20 people injured.

In June 2015, a 21-year-old man armed with a handgun began shooting during a prayer service at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, killing nine people. The shooter fled the scene, and law enforcement apprehended him the next day. He received a death sentence.

In November 2017, a 26-year-old man outfitted in full tactical gear and armed with a rifle exited his vehicle and began shooting outside the First Baptist Church in Sutherland Springs, Texas. He entered the building through a side door and continued firing at the members gathered within. Upon leaving, a neighbor wielding a firearm confronted the assailant, leading to a car chase. Twenty-six people lost their lives, and 20 suffered injuries. The shooter committed suicide. It was the deadliest attack on a house of worship in U.S. history.

In October 2018, a 46-year-old man armed with a rifle and three handguns began shooting inside the Tree of Life Synagogue in Pittsburgh, Pennsylvania. Eleven people died, and six suffered injuries, including four law enforcement officers. Police apprehended the shooter at the scene after exchanging gunfire. Prosecutors charged the perpetrator with committing a hate crime; he is awaiting trial.

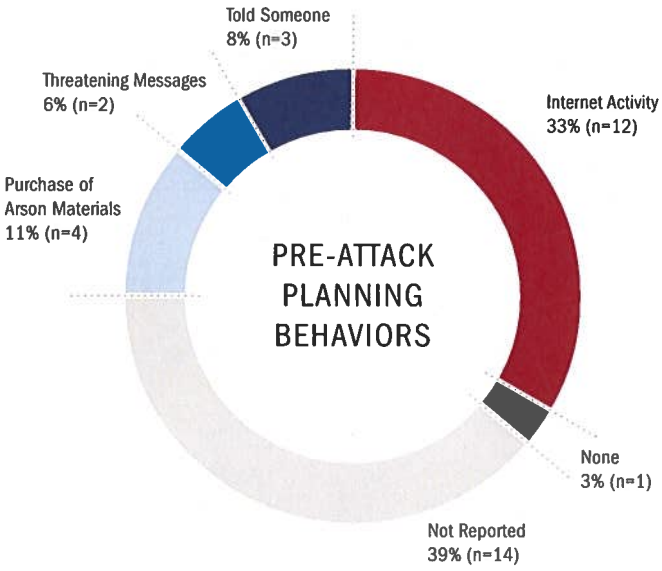


Figure 7. Pre-Attack Planning Behaviors

Figure 7 illustrates the pre-attack planning behaviors exhibited by the perpetrators for the incidents included in the analysis.

Attack Outcomes

As a result of these 37 incidents, 64 people lost their lives, 59 people suffered injuries, and 14 incidents resulted in significant property damage. The number of deaths per incident ranges from 0–27 and the number of injured ranges from 0–20. Active shooter incidents produced the highest numbers of casualties relative to all other types of attacks.

The Perpetrators

CISA identified 36 individual perpetrators across the 37 incidents. Lone actors carried out 30 of the attacks, three conspirators perpetrated one incident, two conspirators perpetrated one attack, and the four cyberattacks had no identified perpetrator. The 36 attackers ranged in age from 17 to 73 years old, with an average age of 38 years. One attacker was female; the other 35 were male. Of the 36 attackers, 67 percent (n=24) were white, 22 percent (n=8) were black, 5 percent (n=2) were Asian, and 5 percent (n=2) were not identified by race in coverage of the incident. CISA used the U.S. Census Bureau standards for defining race in this guide.

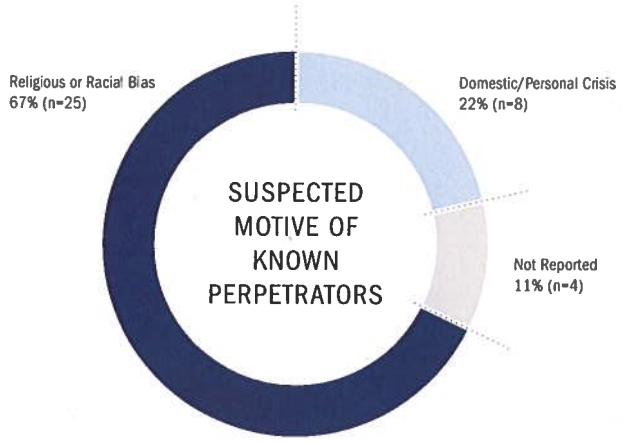


Figure 8. Suspected Motive of Known Perpetrators

Figure 8 depicts the breakdown in the suspected motive for each of the 36 known perpetrators.

Figure 9. Reported Criminal History of Known Perpetrators

Figure 9 shows the number of known perpetrators believed to have a criminal history (58 percent total, n=21), as reported in media accounts, with a further distinction between violent and nonviolent crimes.

Media reports indicate that 58 percent (n=21) of the perpetrators engaged in some form of pre-attack planning behavior that indicated their intent to attack, either by telling someone directly, leaving threatening messages with the HoW, purchasing materials necessary for the attack (such as incendiaries), or describing their plans in an online forum. Figure 7 (p. 21) depicts these behaviors.

CISA concluded that 69 percent (n=25) of the perpetrators (n=36) were motivated by hatred of a racial or religious identity associated with the targeted house of worship. The assailants often revealed specific motivations in comments made during or after the attack, and many self-identified as holding hateful beliefs. CISA determined that 22 percent (n=8) of the perpetrators were motivated by a domestic dispute or personal crisis, including several instances of possible mental health crisis or other individual stressors. Each type of motivation, illustrated in Figure 8, tends to produce different sets of pre-planning behaviors and offers different windows for early detection and intervention, as outlined in later chapters.

A history of criminal activity or mental health struggle can sometimes serve as an indicator of future behavior. Of the 36 individual perpetrators included in these case studies, 21 were identified by family members, witnesses, courts, or media accounts as having a criminal history of some kind, and—based on the reporting of the incident—14 of the individuals are believed to have experienced a mental health struggle either some time before or during the incident. See Figure 9 for a breakdown of perpetrators with a criminal history.

Targeted Houses of Worship

Of the 37 incidents, 54 percent (n=20) targeted Christian institutions, 24 percent (n=9) targeted Muslim institutions, 19 percent (n=7) targeted Jewish institutions, and 3 percent (n=1) targeted Sikh institutions, seen in Figure 10. CISA's analysis found that 65 percent of the attacks (n=25) occurred inside the main building of a HoW; the remaining incidents (n=12) took place at associated facilities such as faith-based community centers, residences, parking lots, or involved HoW computer systems.

During armed assaults (n=20), 40 percent (n=8) of the perpetrators began their attack inside the main building during the worship service. In 45 percent (n=9) of the armed assault attacks, witnesses or members of the congregation attempted to intervene with the perpetrator prior to the arrival of law enforcement.

In 22 percent (n=8) of the total incidents, the perpetrator had some prior association with the HoW, as indicated in Figure 11. In the remaining 78 percent of incidents (n=29), there was no prior association, suggesting the need for a robust and clearly defined greeting protocol as described in Chapter 4.

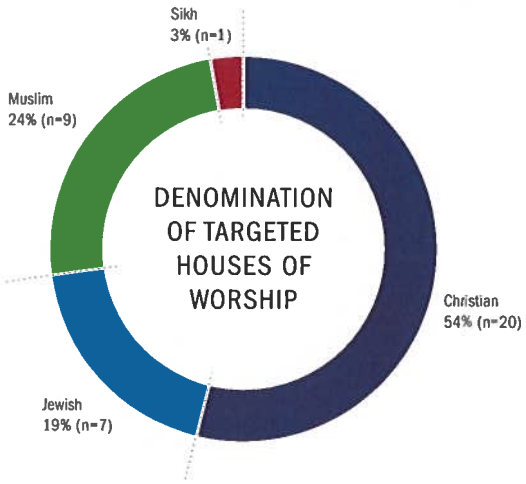


Figure 10. Denomination

Figure 10 shows the breakdown in the denominations of the targeted houses of worship.

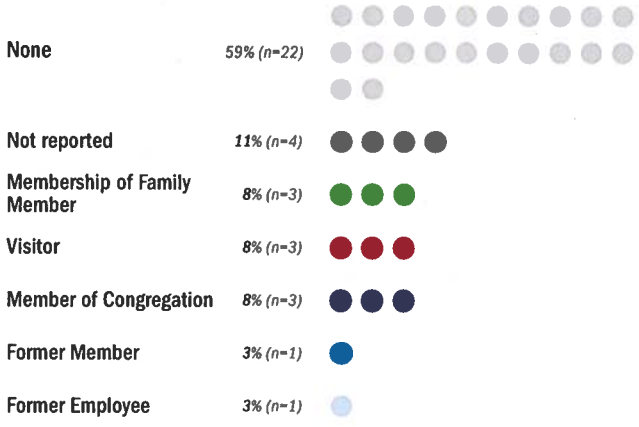


Figure 11. Associations to Facility

Figure 11 shows a breakdown of the number of incidents in which the perpetrator had some prior association with the HoW subject to attack.

Perpetrator Tactics and Methods

As a part of this analysis, CISA examined the tactics and methods used by perpetrators to carry out the attacks. Several of the tactics and methods identified provide insight into efforts a HoW could take to prevent or mitigate potential incidents. These range from specific vulnerabilities exploited by the perpetrator to individual behavioral trends important for a HoW to consider when fostering community engagement.

The following section provides a brief description of several incidents, with a focus on the distinguishing characteristics that houses of worship might consider while revising their security procedures.

PRIOR ASSOCIATION

22% In 22 percent (n=8) of the cases, the perpetrator had some prior association with the HoW.

INCIDENT OVERVIEW

In 2012, a man sought out his ex-wife at their former church. He entered the building during services and fatally shot her as she was playing the organ. The shooter exited the church and returned a few minutes later to fire two additional shots at the victim before he was subdued by witnesses.

INCIDENT OVERVIEW

Over a ten-night span in April 2019, an individual burned down three historically black Baptist churches. The lone actor posted pictures and videos of the crimes to social media in real-time. Emboldened by online reaction to the first two attacks, the perpetrator conducted a third arson, and was arrested after investigators linked evidence of the crimes to cell phone data and recent purchases of gasoline and other flammable materials. The perpetrator pleaded guilty to multiple hate crime and arson charges.

BEHAVIORAL INDICATORS

57% In 57 percent (n=21) of the cases, the perpetrator engaged in some form of planning behavior that revealed their intention to attack.

19% In 19 percent (n=7) of the cases, the perpetrator posted about their plans in on-line forums associated with white supremacy.

ARSONS & BOMBINGS

FIRE-BOMBINGS OCCURRED WHILE CONGREGANTS WERE PRESENT IN THE BUILDING

8% In 8 percent (n=3) of the cases, there was an arson attack while people were present in the building.

INCIDENT OVERVIEW

A 2017 incident took place when assailants broke an exterior window of a mosque and threw a pipe bomb and a mixture of accelerants into the building. At the time of the attack, congegants were in the building for morning prayers; however, the office in which the bomb was thrown was unoccupied and no fatalities or injuries occurred.

ARSON CASES OCCURRING AT NIGHT AFTER SERVICES

24% In 24 percent (n=9) of the cases, an arson attack took place overnight or outside of business hours.

INCIDENT OVERVIEW

In 2017, an assailant broke into a church overnight and spent several hours destroying property, windows, and furniture before setting fires throughout the building. Police were called to investigate a burglary in progress and arrived to find the fire. The fire was quickly extinguished, but the church was badly damaged.

INCIDENT OVERVIEW

An incident in 2014 occurred entirely in the parking lots of two different locations. The attacker first drove to a Jewish community center and began shooting in the parking lot, killing two people. Staff within the facility initiated immediate lockdown procedures, securing exterior doors and ushering visitors to interior rooms. Confronted by an off-duty policeman working security, the attacker drove to a nearby retirement community, where he shot another individual in the parking lot before he was apprehended by law enforcement.

ARMED ASSAULT

ATTACK TOOK PLACE OUTISDE

11% In 11 percent (n=4) of the cases, the attack took place entirely in the parking lot or exterior of building.

SHOOTER MOVED FROM THE OUTER PERIMETER TO INNER SANCTUARY

8% In 8 percent (n=3) of the cases, the attack began at the outer or middle perimeter and moved to the inner sanctuary of the house of worship.

INCIDENT OVERVIEW

During an incident in 2017, the shooter parked outside of a church and waited for services to end. The attacker shot a woman walking to her car before entering the main doors of the house of worship and shooting an additional six people inside the sanctuary. After the incident, renovations included adjustments to the layout to allow congregants to view the main entrance during services.

INCIDENT OVERVIEW

In December 2019, a large group gathered in the home of a New York rabbi to celebrate the end of Hanukkah when a mentally disturbed man entered the home and attacked the gathering with a machete. The congregants fought back, and several people were seriously injured in the ensuing melee; one man later died from his injuries. The attacker fled and attempted to enter the synagogue next door but found the doors locked by people who had heard the commotion. The attacker fled and was later apprehended by police.

ATTACK TOOK PLACE OUTSIDE OF FORMAL SERVICE

14% In 14 percent (n=5) of the cases, the attack took place outside of the primary worship service.

SHOOTER BEGAN ATTACK AFTER THE WORSHIP SERVICE HAD BEGUN

19% In 19 percent (n=7) of the cases, the attack took place during primary worship service.

INCIDENT OVERVIEW

In September 2017, a man armed with two handguns approached a church as services were concluding. Purportedly seeking revenge for the 2015 Charleston church shooting, the man shot and killed one woman in the parking lot. He then entered the building through a rear door and shot and wounded another six people. An usher confronted the gunman, and the gunman accidentally shot himself in the struggle. The usher was able to subdue the wounded shooter until police arrived.

INCIDENT OVERVIEW

In 2019, a gunman entered a house of worship on a major religious holiday armed with tactical gear, an assualt rifle, and at least 50 rounds of ammunition. The assailant shot and killed one person and injured three before the rifle jammed and he fled.

ASSAILANTS TARGETED HoWS DURING PERIODS OF INCREASED ATTENDANCE (E.G., HOLIDAY SERVICES)

22% In 22 percent (n=8) of the cases, the attack took place on or around a religious holiday.

SHOOTER SAT THROUGH THE SERVICE BEFORE THE ATTACK

8% In 8 percent (n=3) of the cases, the attack took place after the perpetrator sat through part of the worship service.

INCIDENT OVERVIEW

In a 2019 incident, the shooter sat through part of the worship service before standing with a shotgun and fatally shooting a person nearby. The assailant wore an obvious disguise and his suspicious behavior drew the attention of the HoW volunteer security team, who responded immediately and subdued the attacker.

INCIDENT OVERVIEW

During a 2012 religious holiday, a house of worship was the victim of a cyberattack in which an unknown actor vandalized the HoW's homepage and redirected visitors to a site expressing support for a well-known terrorist group. The website defacement included upsetting images and boastful messages from the cyber actors.

CYBER ATTACK

WEBSITE DEFACEMENT

5% In 5 percent (n=2) of the cases, the attack involved the defacement of a HoW website.

FINANCIAL EXPLOITATION

5% In 5 percent (n=2) of the cases, the attack involved a financial exploitation.

INCIDENT OVERVIEW

In 2019, a phishing campaign targeted a house of worship by spoofing a vendor's email and redirecting the HoW's monthly payments to a fraudulent account. The attack resulted in a significant financial loss and was only discovered when the "real" company called to ask about late payments.

TACTICS & METHODS

Tactic or method	% of incidents	Recommendations	Description of Events
BEHAVIORAL INDICATORS			
Perpetrator engaged in planning behavior indicating their intention to attack	**57%** (n=21)	Suspicious Activity Training **Chapter 4**	Over half of the perpetrators revealed their intention to attack through action or word.
PRIOR ASSOCIATION			
Perpetrator had some prior association with the HoW	**22%** (n=8)	Greeter Training Wellness Programs **Chapter 4**	A susbstantial number of attackers were known to members of the HoW community, but the majority had no previous association.
ARMED ASSAULT			
Attack took place outside	**11%** (n=4)	Access Control **Chapter 5**	The assaults, which included both active shooter incidents and vehicular attacks, took place entirely in the parking lot or exterior of the HoW building.
Shooter sat in the service before attack	**8%** (n=3)	Greeter Training **Chapter 4**	In each case the assailant sat through part of the service before attacking congregants.
Shooter moved from outer to inner perimeter	**8%** (n=3)	Active Shooter Training & Access Control **Chapter 4, 5**	In each case the assailant began shooting in the parking lot and continued the assault while moving into the interior of the main sanctuary.
Shooter began attack inside the main building during the worship service	**19%** (n=7)	Active Shooter Training **Chapter 4**	The assailants entered the main building with the sole purpose of harming congregants, either indiscriminately or because their individual target was known to be there.
Assailant attacked during periods when larger than normal attendance was expected (e.g., holiday services)	**22%** (n=8)	Increasing Security During Busy Events **Chapter 4**	Perpetrators planned these attacks around a high volume of congregants.
Attack took place during non-worship activities (e.g., partner groups, community theater)	**14%** (n=5)	**Chapter 4**	Assailant chose to attack congregants during small group gatherings.
ARSONS & BOMBINGS			
Bombing occured while congregants were present in the building	**8%** (n=3)	Suspicious Activity Training **Chapter 4**	Perpetrators intended to harm as many of the congregants as possible by attacking during worship services.
Arson cases that occurred at night after services	**24%** (n=9)	Exterior Lighting Visible CCTV **Chapter 5**	Most of the arson cases occurred after business hours and often resulted in substantial property damage.
CYBER ATTACK			
Financial Schemes (e.g., Ransomware, Phishing)	**5%** (n=2)	Cyber Resilience **Chapter 7**	Financial schemes resulted in almost $2.5 million in losses.
Website Defacement	**5%** (n=2)	Cyber Resilience **Chapter 7**	In both instances, perpetrators defaced websites to show support for foreign terrorist groups.

Security in Practice

In the following chapters, CISA highlights general best practices and examples from the case studies where HoWs had the tools and procedures in place to respond effectively as the attacks unfolded. A few facilities had designated security directors and established formal training programs; another had a volunteer security team that conducted regular emergency response drills and was credited with protecting fellow congregants during the incident. Some facilities initiated lockdown procedures after the attacks began. In several cases, active shooter training saved lives because leaders and congregants knew how to respond and helped others escape or hide. Look for the 'Security in Practice' call out boxes with examples of lessons learned and best practices.

Based on the identified tactics and methods, CISA's recommendations for HoWs contain many tangible guidelines for developing a layered security strategy, conducting vulnerability assessments, developing an organizational safety culture, enhancing physical security, strengthening cybersecurity readiness, and developing guidance for daycare and school safety where applicable.

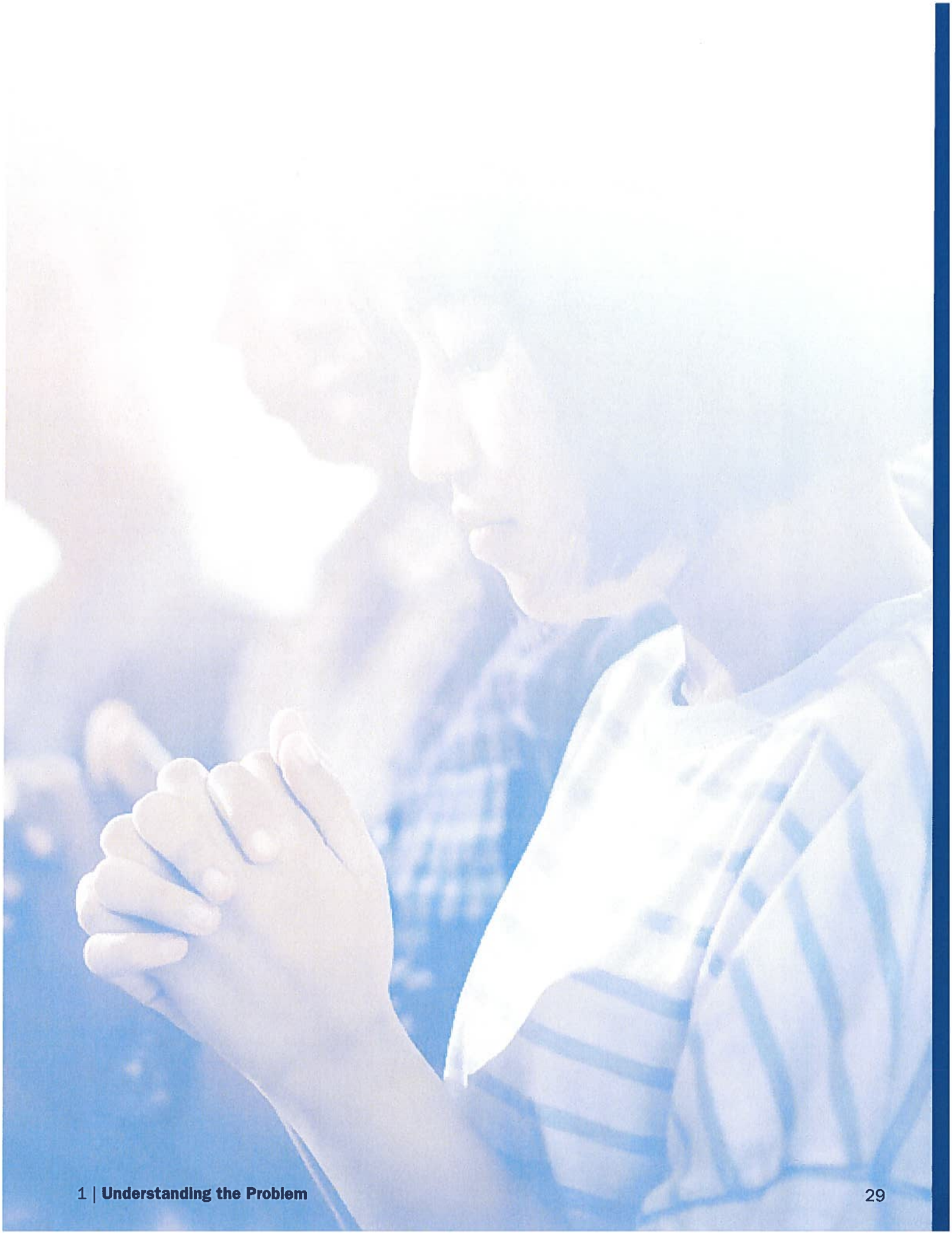
SECURITY IN PRACTICE

EMERGENCY ACTION PLANNING

In the aftermath of one attack, an affiliated community center provided critical support to victims and families within hours. Community center leaders stressed that having an an emergency response plan already in place was essential to sheltering and caring for the victims.

Summary

The case studies examined here provide a snapshot of targeted violence against HoWs that have occurred in the United States over a ten-year period. Though statistically rare, each was a moment of profound trauma for both the victims and society at large. However traumatic, each event also presents an opportunity to learn—about the forces that shape American society, the motivation of the attackers, and, most importantly, about the steps that houses of worship can take to better protect life and property.



2 Developing a Holistic Approach to Security

Introduction

Experts consistently stress the need for houses of worship (HoWs) to take a layered and holistic approach to security.[1] That task might seem like a daunting—and potentially expensive—prospect for communities that lack special expertise. However, developing a comprehensive security strategy is relatively simple with the right frame of reference, and the Cybersecurity and Infrastructure Agency (CISA) is here to help.

In this chapter, CISA provides a framework for thinking about the security of your HoW and to begin planning for the future.

Security planning is a complex balancing act between cost, culture, and need. The most reliable way to resolve those competing demands and make sound, cost-effective decisions is to develop a plan that rests on a strong understanding of security planning basics and the unique challenges that exist at every house of worship.

What is a Holistic Approach to Security and How Do You Get There?

Security professionals sometimes talk about the concept of *enterprise security*, a term most commonly used in the cyber domain. In practice, it simply means taking a comprehensive approach to the security needs of an entire organization.

An effective security program is never one-dimensional.

Another way to think about this idea is to consider the security of your HoW as a holistic endeavor that relies on the sum of its parts and encompasses all the different aspects of your buildings, community, and activities. Each of those aspects and activities of your organization needs some measure of protection. At the same time, it is also important to be aware of the various threats, risks, and vulnerabilities that might be present at your HoW.

1 Hady Mawajdeh, "Experts Encourage Layered Approach to Church Security Protocols," *NPR*, January 3, 2020; Scott Stewart and Fred Burton, "Security at Places of Worship: More than a Matter of Faith," *Stratfor*, June 17, 2009.

In practice, moving toward a solution and developing a holistic security strategy means considering (or perhaps revisiting) the range of measures necessary to keep your house of worship safe, including physical security, cybersecurity, community awareness, event planning, incident management, emergency preparedness, policy development, training, and human resources.

The rest of this chapter outlines the key concepts, considerations, and distinct steps that will help you to develop a robust, inclusive, and multilayered approach to security.

Key Concepts, Terms, and Questions

The array of measures that might be necessary to keep your congregation safe can appear overwhelming. Start by asking a series of basic questions that will help to clarify your current security posture and any changes that might be needed:

- **What are your threats and vulnerabilities?**
- **What is the likelihood of any given threat to occur?**
- **What are the consequences if those threats occur?**
- **What is your community's tolerance for the associated consequences?**
- **What is your community's attitude toward security practices?**
- **What personnel resources do you have to direct, manage, and oversee security operations?**
- **What is your budget to support security initiatives, both immediate and long-term?**

Questions such as these inform any kind of enterprise security project. Houses of worship also face additional special considerations due to the unique nature of the threat environment and the general preference for maintaining an open, peaceful, and welcoming atmosphere.

As you set out on this process, it's important to consider some of the following dynamics to inform your overall strategy and approach:

RISK, THREAT, VULNERABILITY, AND CONSEQUENCE

Risk, threat, vulnerability, and consequence all have important distinctions that you should bear in mind as you develop your security strategy. You might think of the relationship between them as: ***risk = threat × vulnerability × consequence***.

The Department of Homeland Security (DHS) specifically defines these terms as follows:

RISK: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Risk is a function of threat, vulnerability, and consequence.

THREAT: natural or man-made occurrence, individual, entity, or action that has or indicates the capability and intent to harm life, information, operations, the environment, and/or property.

VULNERABILITY: physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

CONSEQUENCE: effect of an event, incident, or occurrence.

U.S. Department of Homeland Security, *DHS Risk Lexicon, 2010 Edition* (September 2010), https://www.cisa.gov/dhs-risk-lexicon

THE UNIQUE NATURE OF TARGETED VIOLENCE AGAINST HoWS. As sites of religious practice, houses of worship have major symbolic importance within their community and, as such, can draw hostile attention from would-be perpetrators. CISA's analysis strongly indicates that ideology or personal crisis motivates most incidents of targeted violence against HoWs, some of which may be subject to early detection and intervention.

AWARENESS OF THREATS. Most houses of worship are generally attuned to the rhythms and attitudes of the communities they serve and are a critical part of the social fabric. Embracing that role can be a major asset in improving security by improving awareness of social tensions or personal crises that might herald a violent incident.

THE ABILITY TO INTERVENE AGAINST SUSPECTED THREATS. While community engagement is the best way to improve awareness, formal partnerships—with other houses of worship (including those of different faiths), community groups, law enforcement, and social service providers—are often necessary to act against a potential threat. You should evaluate the kind of formal partnerships your HoW maintains as part of this process.

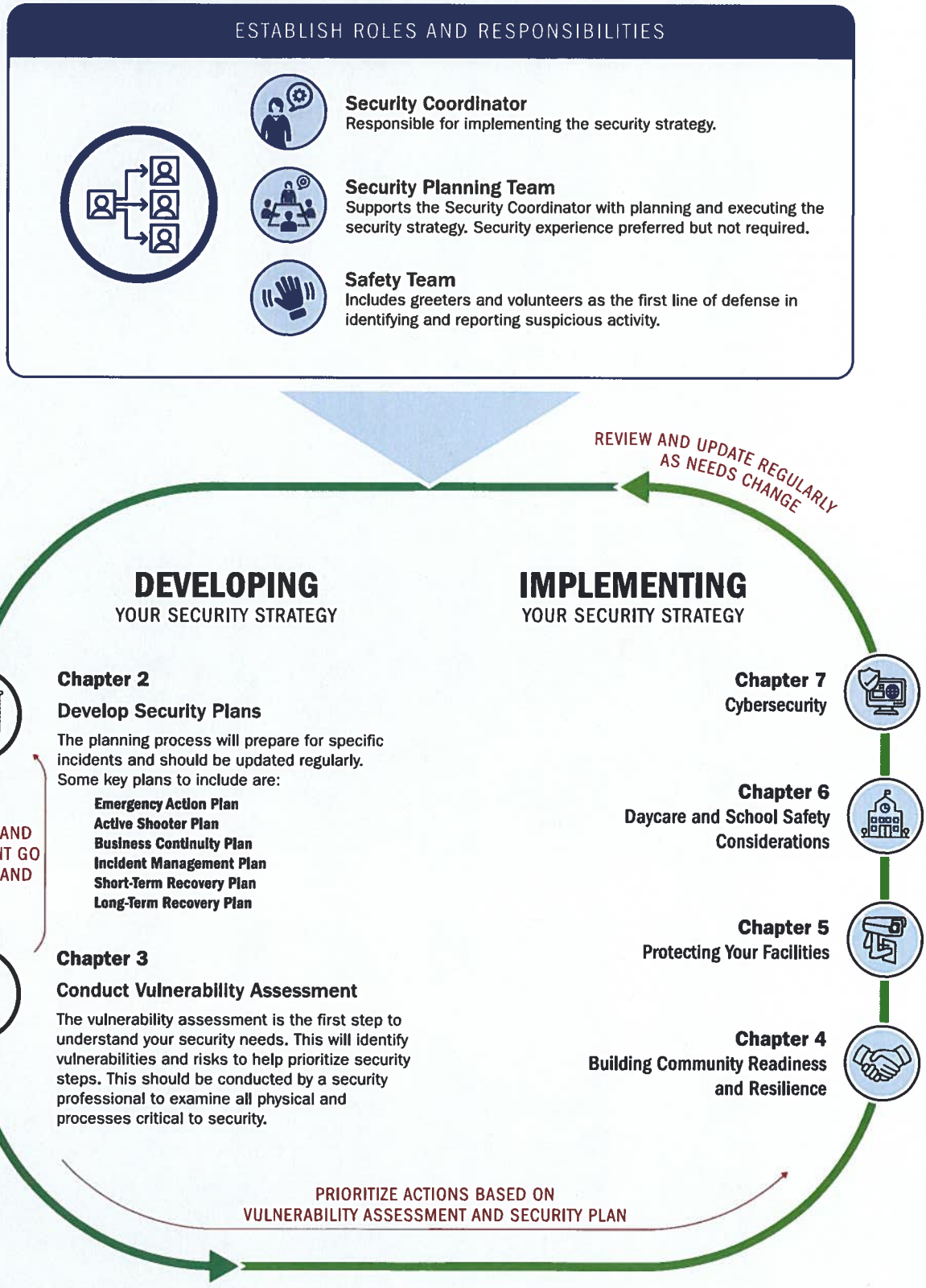
THE BALANCE BETWEEN CONVENIENCE, OPENNESS, AND SECURITY. No house of worship wants to be a fortress. You will have to decide for yourself—in collaboration with your community and in accordance with your values—how to strike the balance between creating a secure environment and an open one. The choice, however, is not absolute, and the framework offered in this guide is intended to help you strike the balance that is right for your house of worship.

These are complex issues that require internal deliberation, philosophical discussion, cost-benefit analyses, and ultimately, consensus building among key stakeholders within every house of worship. The bottom line is that an effective security program is never one dimensional and best achieved through a constant process of discussion and (re)evaluation.

Look for the red arrows throughout the report highlighting sources for further information

A good place to begin thinking about these special considerations is with CISA's HOUSES OF WORSHIP: HOMETOWN SECURITY REPORT SERIES (May 2017), which offers specific guidance on how religious communities can Connect, Plan, Train, and Report to improve safety. CISA continues to develop a SUITE OF SECURITY RESOURCES for faith-based organizations (FBOs) and HoWs.

Security Framework for Houses of Worship



Framework for Developing a Holistic Security Strategy

CISA recommends several important steps throughout the rest of the guide for a house of worship to achieve a holistic security strategy. This process starts by establishing clear roles and responsibilities for implementing security procedures and requires regular evaluation.

Getting Started: Establishing Roles and Responsibilities

Establishing clear roles, responsibilities, and expectations is critical for success. The first step in developing a holistic security strategy is to determine who will oversee the program. Although specific duties and titles may differ according to the unique circumstances of every HoW, this person—the *Security Coordinator*—is typically the primary decision maker for security related questions and charged with overseeing the day-to-day details of the security program. Ideally, this will be a full- or part-time staff member or engaged volunteer with relevant professional experience.

Planning is one of the most important parts of the process.

CISA recommends forming a *Security Planning Team* to support the Security Coordinator by conducting research, evaluating needs, providing recommendations, and assisting with plan development. This group should be representative of the HoW and include clergy, staff, and members of the congregation. The Security Planning Team can serve a variety of purposes and should help carry the burden of planning and implementation.

When identifying candidates for these positions, consider surveying your staff and members to identify in-house professionals whose experience could inform the planning process. For example, if the community has security, law enforcement, mental health, emergency preparedness, or incident management professionals, their knowledge and expertise can bolster your efforts and help build formal partnerships. Other valuable skill sets include policy development, strategic planning, finance and accounting, and training. One of the challenges is to design a process that encourages critical thinking and innovation while delegating authority to avoid overburdening volunteers.

In addition, CISA encourages HoWs to account for the safety and security considerations for the wider range of people affiliated with the HoW, such as congregants, volunteers, greeters, ushers, and maintenance staff, etc. This group can constitute a larger *Safety Team* to assist in carrying out the safety and security program. While most of the decision making would fall to the Security Coordinator and Security Planning Team, the Safety Team is instrumental in creating a wider culture of security and ensuring that the entire HoW community is involved in the general conversation around safety. This could include everything from how greeters look to identify suspicious activity, to identifying who is responsible for locking doors when there are no activities occurring.

The Planning Process

An effective security strategy takes time to develop and implement, and planning is one of the most important parts of the process. The goal is to develop a long-term comprehensive strategy, so it is more important to move through each step in a thoughtful and deliberate manner than it is to move quickly.

There are two main activities that go into the planning stage and they go hand-in-hand. The primary goal at the start of this process is to identify your vulnerabilities and begin developing a plan to address them.

The needs of every house of worship are different.

The *Vulnerability Assessment* is further detailed in Chapter 3 and will help you identify the specific threats that might exist in your community and your exposure to certain risks. The vulnerability assessment is the first step in the planning process; the next step is to begin making plans to address those vulnerabilities and to implement a dynamic and multilayered security strategy.

The vulnerability assessment and planning process are distinct tasks but are closely linked. Each informs the other and, in many respects, the process never ends because a key feature of a responsive security strategy is to reevaluate your needs and adjust your plans on a regular basis.

As you move forward in the larger planning process and begin implementing your security strategy, you may also want to consider developing a number of related plans for specific kinds of situations and incidents. For more information on advanced planning, see Chapter 4.

Components of a Holistic Security Strategy: How to Secure Your House of Worship

The planning process is part of a long-term cycle and strategy, and the vulnerability assessment is likely to reveal a (potentially long) list of needs and wants. Some of those can be addressed immediately, but others will take time. All of your plans will require some level of organization and prioritization. This guide is intended to help you make those necessary judgments.

Each of the remaining chapters of this guide discusses a different key component of a holistic security strategy and highlights federal resources wherever possible, all with an overall emphasis on developing a thoughtful, inclusive, and multi-layered approach to security planning.

CHAPTER 3 provides further details and guidance on how to conduct a comprehensive *Vulnerability Assessment*, which will help you to understand the ways in which your HoW might be exposed to risk.

CHAPTER 4 describes how *Building Community Readiness and Resilience* can offer protection by educating your community, building partnerships, and making changes to the general practices and behaviors within your house of worship.

CHAPTER 5 offers a framework for *Protecting Your Facilities* and encourages HoWs to think about how physical security can be improved by making changes along the outer, middle, and inner perimeters of the property, grounds, and buildings.

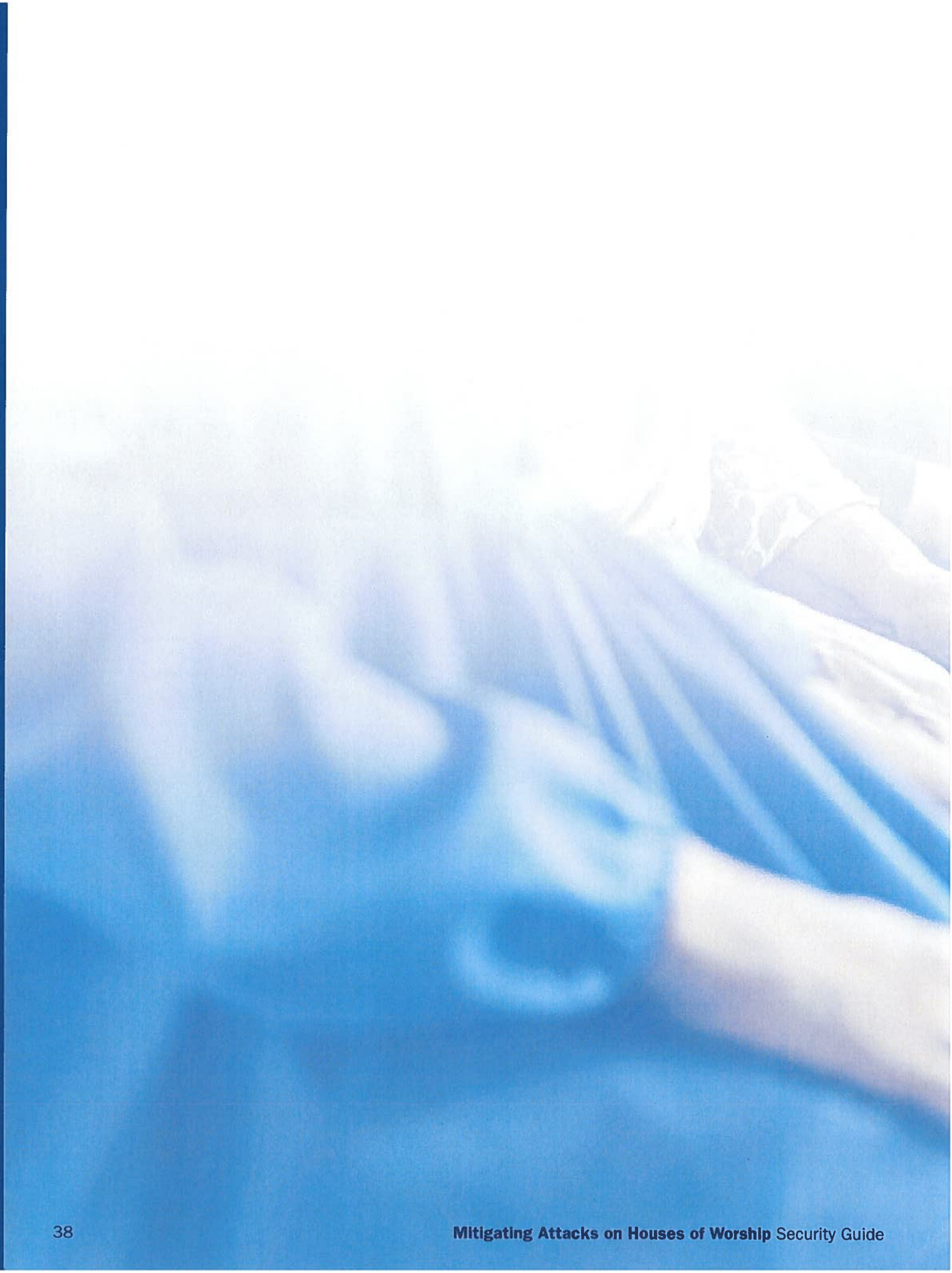
CHAPTER 6 outlines the special care that should go into *Daycare and School Safety Considerations* wherever applicable.

CHAPTER 7 offers a primer on *Cybersecurity* for houses of worship. This is often an overlooked vulnerability but one that can be addressed and mitigated by developing a culture of cyber hygiene and applying a number of readily available free resources.

Finally, **APPENDIX 1** presents a *Resource Guide* with a comprehensive list of products that can be used to improve the overall safety and security of your house of worship.

Summary: Achieving a Holistic Security Strategy

Security planning is a complicated endeavor and the needs of every house of worship are different. CISA's purpose is not to make this guide a single source, all-inclusive manual, but rather to provide a comprehensive framework for developing a sound and holistic security strategy. Although the chances of your house of worship suffering an attack are small, the preparations described here can save lives and apply to a range of emergency scenarios should an incident ever come to pass.



3 Conducting a Comprehensive Vulnerability Assessment

Introduction

Performing a comprehensive vulnerability assessment is a critical step in the development of a robust security program, and the process is just as important as the findings. The assessment described here identifies existing safety features and practices, determines current threats and vulnerabilities, and highlights areas for improvement.

The assessment should consider the threat landscape that is unique to every house of worship (HoW) and weigh the possibility of scenarios involving active shooters, vehicle rammings, improvised explosive devices (IED) or vehicle-borne IEDs (VBIED), arson, edged weapons, and cyberattacks, to name just a few. HoWs with onsite school or daycare facilities should be aware of unique challenges associated with educational institutions and see Chapter 6 for specific guidance for safeguarding these types of facilities.

The Vulnerability Assessment Model provided in this chapter and the Cybersecurity and Infrastructure Security Agency's (CISA) HoW SECURITY SELF-ASSESSMENT tool support a systematic approach to this process. Organizations of all types and sizes can leverage these and other available tools and resources to customize an assessment process, develop a robust security strategy, and guide the allocation of personnel and financial resources to implement that strategy. Evaluating the assessment results on a recurring basis will help address evolving threats and ensure security measures are responsive to the current threat environment.

Assign Roles and Responsibilities

Conducting a vulnerability assessment begins with deciding who will lead the process. An organization's size, location, and available resources are all major considerations that can shape a vulnerability assessment and should factor into decisions about who assumes this role.

Ideally, the Security Coordinator will lead this process with support from the Security Planning Team. Shared decision-making responsibilities will help ensure the results represent a consensus view and that any changes resulting from the assessment will have the support of the HoW community.

If the security challenges seem relatively straightforward—such as for a small, rural HoW—the vulnerability assessment can likely be performed in-house.

CISA PROTECTIVE SECURITY ADVISORS (PSAs)

PSAs are subject matter experts specially trained in vulnerability mitigation and critical infrastructure protection. PSAs facilitate local CISA field activities in coordination with other Department of Homeland Security (DHS) offices. They also advise and assist state, local, and private sector officials, as well as critical infrastructure facility owners and operators. PSAs frequently conduct vulnerability assessments for houses of worship and schools.

For additional details on PSAs, visit HTTPS://WWW.CISA.GOV/PROTECTIVE-SECURITY-ADVISORS or contact CENTRAL@CISA.DHS.GOV.

Assessments involving more complex security environments—such as at a megachurch, a dense urban area, or a HoW that is particularly prominent—might consider reaching out to a CISA PSA to help design a tailored process that can be carried out by a team of volunteers.

Determine the Scope of Your Vulnerability Assessment

Tailor the vulnerability assessment to your organization's specific interests and needs. To determine the scope and complexity of an assessment, consider some of the following questions:

- **Why are you conducting this assessment now?**
- **Have you previously conducted any similar assessments? If so, how did you use the findings and recommendations?**
- **Have you already identified specific threats or vulnerabilities? Has your organization experienced threats or incidents of violence in the past?**
- **How does the location and size of your HoW affect your security concerns?**
- **Is your local community facing safety and security concerns that could impact your HoW community?**
- **Do you have a budget for security measures? If not, will there be budget planning opportunities for security in the future?**

The answers to these questions will help define the scope of your assessment and develop a process that accounts for all aspects of your organization's security posture. Ideally, this will lead to clear evidence-based decision-making about priorities, wants versus needs, short- and long-term goals, budget considerations, and feasibility. In many cases, this process will result in action items that are relatively easy to implement. Other findings may be more complex and require engaging with outside resources, such as CISA PSAs.

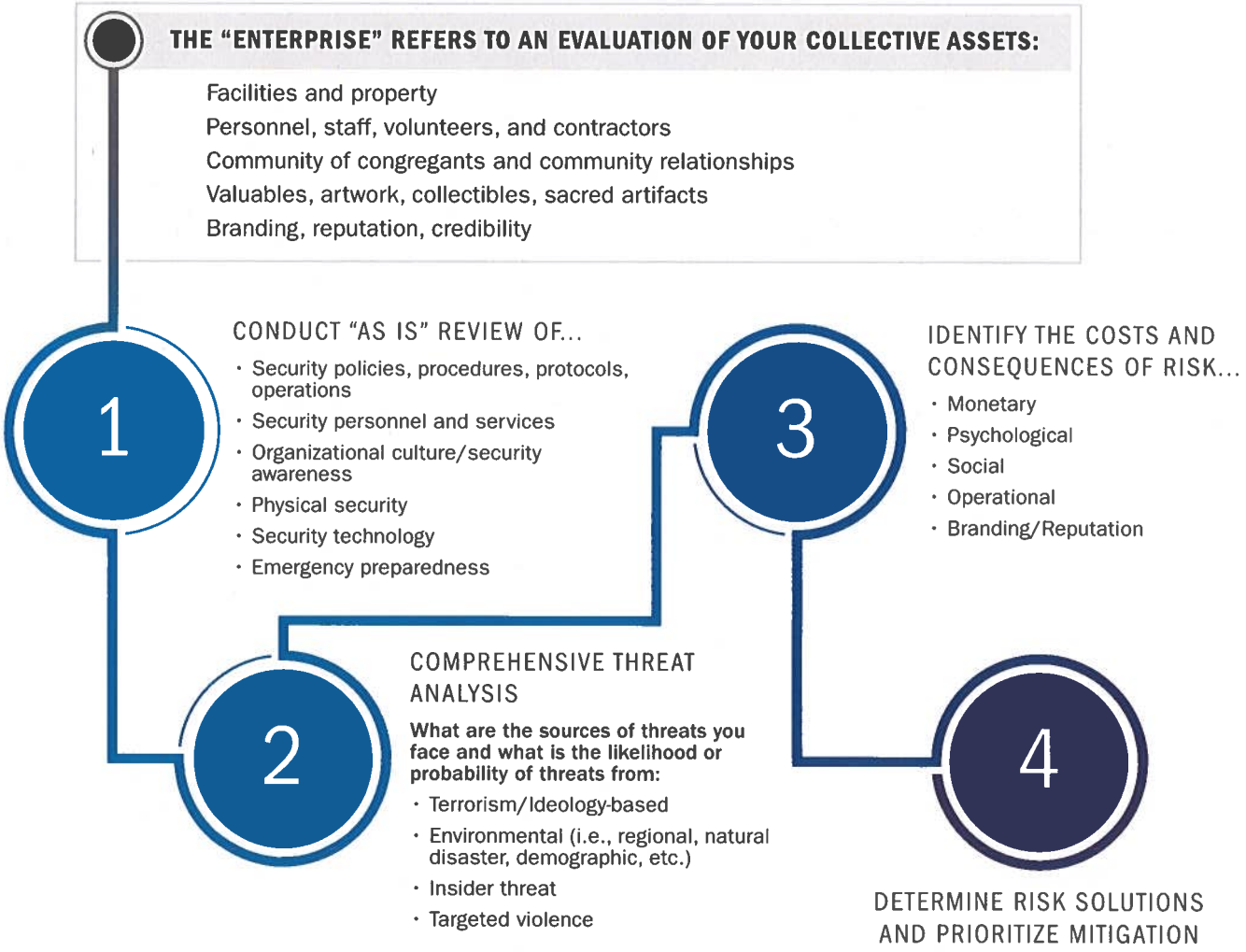
A Vulnerability Assessment Model

A systematic approach is essential to producing a high-quality assessment. This vulnerability assessment model examines an organization's functional areas to generate findings that can be evaluated in the context of feasibility, complexity, expected benefits, cost, and resource availability.

To enhance this process, CISA has developed a HOUSE OF WORSHIP SECURITY SELF-ASSESSMENT tool with a series of questions designed to uncover vulnerabilities and areas for improvement. This tool can also serve as a template that can be tailored to align with specific organizational needs. Alternatively, a CISA PSA or other consultant can provide additional guidance for conducting a self-assessment.

This type of assessment typically involves collecting data and information through interviews with key personnel and stakeholders, performing on-site inspections and observations, reviewing records and materials such as existing security and training plans, and examining public records such as local crime statistics.

The most important aspect of an assessment is to document your process and findings so that the process itself can be replicated and the data can be used to develop a security strategy.



Key Considerations for Leveraging the Vulnerability Assessment Model

Organizational Assets

IDENTIFY FACILITIES AND PROPERTY

Identify and describe your facilities:

- **Identify each of the buildings on your property, such as the main HoW building, chapel, rectory, school, playground, community center, and parking.**
- **Describe the number, physical design, and construction of buildings, including year and type of construction, and geographic footprint.**
- **Define the type and number of services held, as well as the schedule and number of congregants that might use each building at any given time. Identify administrative office hours (days and times). List any distinguishing features that might help identify the HoW property.**

*Refer to **Chapter 5** for guidance on physical security and associated resources.*

Define your property in terms of outer, middle, and inner perimeters.

- **Outer perimeter generally includes the parking facility and lots, exterior common grounds, walkways, playgrounds, and the physical façade of the buildings.**
- **Middle perimeter is a fluid area that generally refers to anything that is "on campus" but outside of the main buildings and includes exterior features such as walkways, doors, and walls.**
- **Inner perimeter is any interior space, such as the vestibule, worship area(s), administrative offices, community room, auditorium, and classrooms.**
- **Create a list of all outer, middle, and inner perimeter elements.**

IDENTIFY ASSETS AND VALUES

Identify any valuables that require protection and potential cost of replacement:

- **Determine asset values, costs to protect assets (mitigate risk), costs to replace assets, and costs linked to the organization's reputation and existence if assets are lost.**
- **Identify valuables, such as artwork and sacred artifacts.**
- **Assign a cost for valuables, which can be evaluated as simply "high," "moderate," or "low."**
- **Make informed decisions about investing in protecting or mitigating risk to each asset.**

Conduct As-Is Review

1

REVIEW ADMINISTRATIVE PRACTICES AND SECURITY-RELATED PROTOCOLS

Examine day-to-day operations and relevant administrative procedures:

- **What are your practices around visitor access?**
  - Do you maintain regular business hours?
  - Are any spaces regularly kept locked or open?
  - Is there a protocol for greeting and screening visitors during worship? Is there a protocol for greeting and screening visitors during non-worship hours?
  - Are existing protocols consistently enforced and reviewed on a recurring basis?
- **Do you have emergency action or security plans in place? Do they cover a variety of scenarios, such as for active shooter, emergency preparedness, emergency evacuation, threat assessment, and school security scenarios?**
- **Have you documented all administrative processes, procedures, policies, directives, and operational manuals? Are these policies reexamined and refreshed on a routine basis?**
- **Who oversees financial operations, including offerings and collections? Do you use accounting software? Is there a system for conducting audits and oversight?**

EXAMINE HUMAN RESOURCE PRACTICES

Examine your human resource practices:

- **Does your organization use contract security personnel, either armed or unarmed, to support HoW activities and events? If so, what is their role and does their presence align with current security concerns in the community? Do the security personnel meet all state and local licensing, training, and insurance requirements?**
- **Do you have formalized relationships and partnerships with local law enforcement and/or first responders who have authority in your jurisdiction? Do you meet with them regularly to exchange information and collaborate around security and risk mitigation priorities?**

Refer to Chapter 4 for information on human resource practices.

- **What pre-employment screening protocols do you follow? Are employees and volunteers subject to background investigations, especially those who occupy sensitive positions, such as interacting with children, money, computer systems, or confidential information?**
- **Do current pre-employment screening processes meet standards of practice for comparable positions of responsibility? For more information, refer to the U.S. Equal Employment Opportunity Commission guidance on BACKGROUND CHECKS.**

KNOW YOUR PEOPLE AND YOUR ORGANIZATIONAL CULTURE

Consider your community's attitude toward security procedures:

- **Is your membership generally aware of security best practices, such as "If You See Something, Say Something®" to observe and report suspicious activity?**
- **Do organization leaders share regular and consistent messaging around security and safety, or is this a topic that has not yet been proactively addressed?**
- **Have HoW personnel and/or members participated in formalized training for emergency evacuations, active shooter incidents, or other major events?**
- **Do you have an established process for sharing concerns about suspicious or concerning activities?**
- **Do HoW members and the surrounding community support a security strategy that includes potential security enhancements?**
- **What threats or vulnerabilities are members concerned about?**
- **How do organizational values and initiatives, such as supporting vulnerable populations and providing food, shelter, and social support in the community, align with perspectives on security measures?**

Refer to Chapter 4 for information about organizational culture.

Comprehensive Threat Analysis

2

ASSESS THE THREAT ENVIRONMENT

Establish a baseline awareness of the threat environment:

- **Consider such factors as your organization's public profile and visibility in the community and region.**
  - For example, understand whether ideological, social, or political opinions or beliefs linked to the organization and/or HoW leaders could incur a high level of attention and risk.

- **Analyze a wide range of threats (for example, terrorism or ideology-based threats) relative to probability of occurrence based on location, membership, history of violence, and prominence.**
  - Not all targeted violence is ideologically driven. Some active shooter incidents have been linked to domestic violence, workplace disputes, and mental health crises.
- **Consider how location and proximity might influence your threat environment. For example, degree of risk may increase if a HoW is located next to an organization that is regularly the focus of public attention or targeted for violence or vandalism.**

UNDERSTANDING THE FULL SCOPE OF RISK STARTS WITH:

- **Identifying/listing each type of threat or risk.**
- **Rating and ranking probability of occurrence and impact (e.g., low probability/high impact).**

Identify Risk-Related Costs and Consequences

UNDERSTAND RISK-RELATED COSTS AND CONSEQUENCES

Conduct a risk analysis that clearly identifies consequences associated with identified risks, which can include:

- **Tangible losses, such as money, property, and valuables;**
- **Social, emotional, interpersonal, and psychological damages that may disrupt HoW operations and business continuity; or**
- **Impact to a HoW's brand, credibility, or reputation among stakeholders and throughout the community.**

DETERMINE RISK TOLERANCE

Discuss your community's tolerance for risk:

- **Engage in candid discussions about tolerance for each identified risk. Perspectives related to risk factors, risk tolerance, and risk mitigation can evolve over time; therefore the process for assessing risk and determining risk tolerance should be flexible.**

Determine Risk Solutions and Prioritize Mitigation

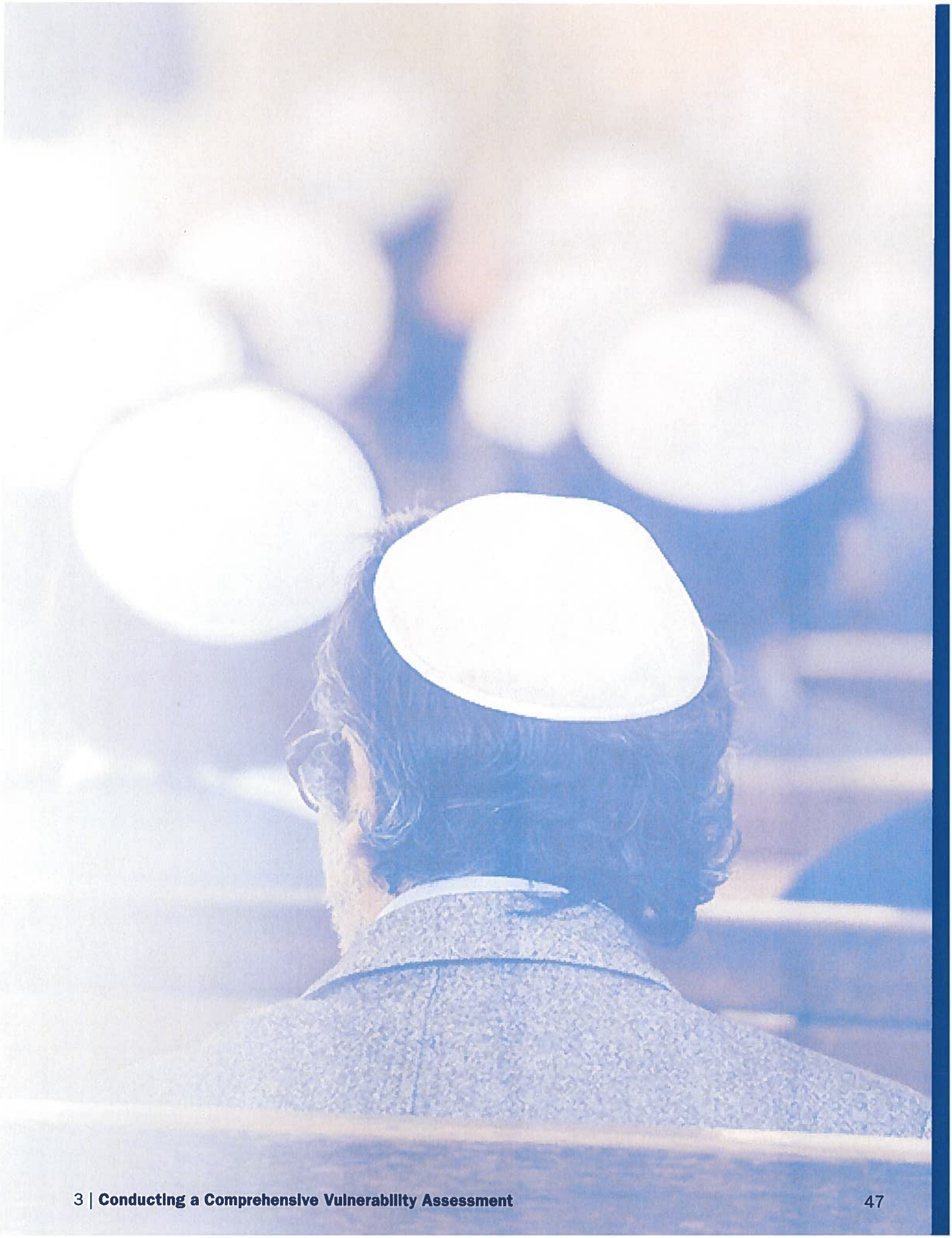
ESTIMATE THE LIKELIHOOD OF A RISK TO OCCUR

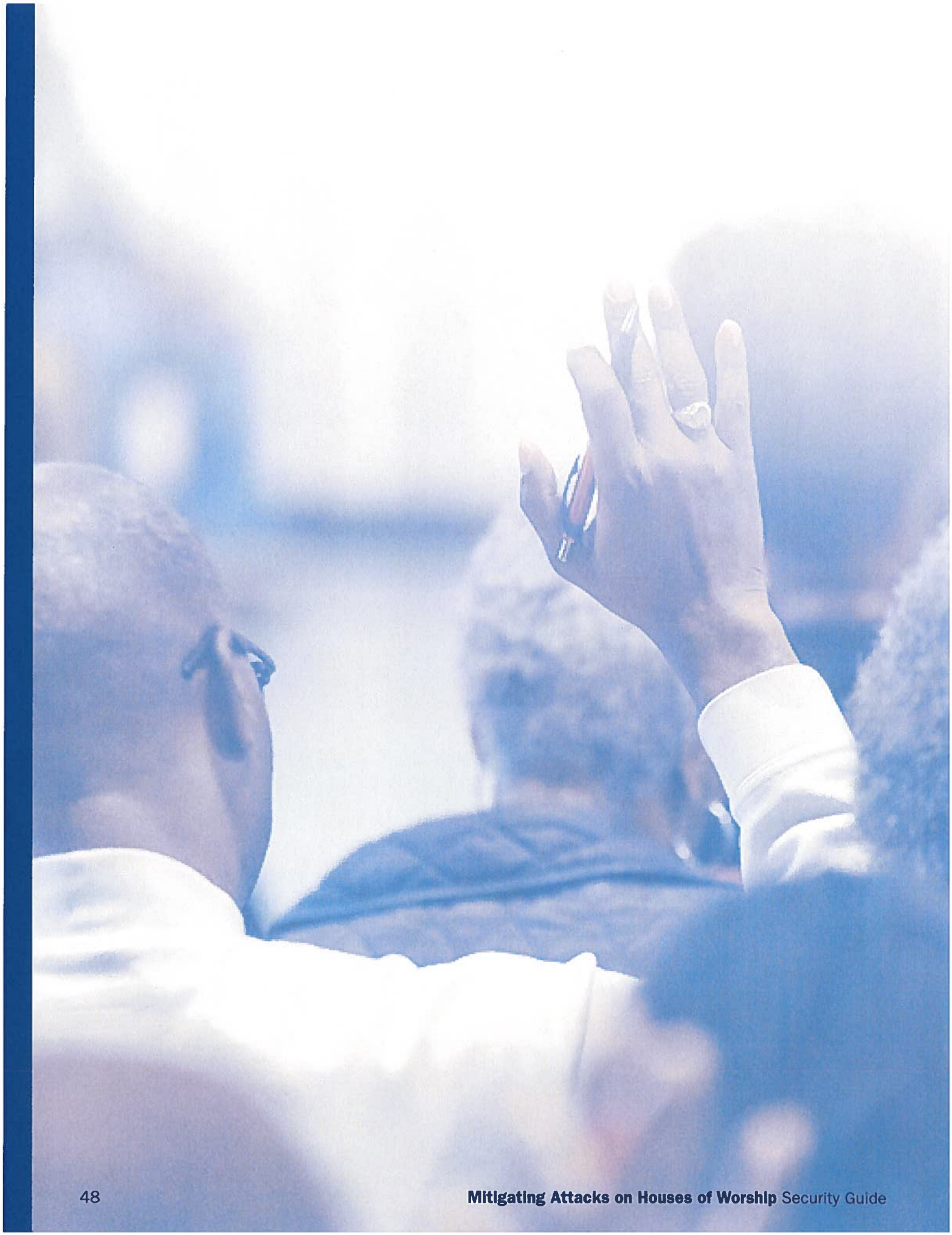
Consider a range of possible scenarios and outcomes:

- **For each risk, estimate the probability of the threat to occur and weigh it against the potential cost and impact associated with that risk.**
  - More complicated risk methodologies can be used. This rating will help prioritize your mitigation strategies and inform security planning.
  - Risks with a high probability of occurrence and associated costs should be ranked as high priority in the overall security strategy.
- **Mitigation solutions can be correlated to risks as:**
  - High need to mitigate
  - Moderate need to mitigate
  - Low need to mitigate

Summary

This chapter provides a framework for designing and conducting a comprehensive vulnerability assessment. Houses of worship can customize these tools and recommendations to assess organizational assets and associated values, identify a threat environment, analyze risk and mitigation solutions, and understand the consequences associated with identified threats. Ultimately, the breadth and depth of a vulnerability assessment is based on resources, feasibility, and the urgency with which you need to address your security concerns. Assessment results should guide discussions about prioritizing specific actions that will shape the organization's security strategy, including how that strategy can be implemented.





4 Building Community Readiness and Resilience

Introduction

People are the most important asset for your house of worship (HoW) to protect—and your best protection against potential threats. This chapter focuses on the people that comprise your HoW community and the relatively simple changes to the way your HoW operates, internally and within the wider community, that can improve your overall security posture.

Human behavior, interpersonal relationships, and community values all play a significant role in security. With the right tools, people can be the first line of defense in identifying suspicious behavior and activities.

This chapter outlines a number of policies and programs that can be implemented with minimal capital investment. Below you will find sections covering internal programs that individual HoWs can implement on an independent basis, specialized policies to consider as you build your overall security program, and ways to connect with the wider community to foster overall awareness, readiness, and resilience.

In the end, building a culture of safety and responsibility is one of the best ways for houses of worship to prepare and respond to any potential acts of targeted violence.

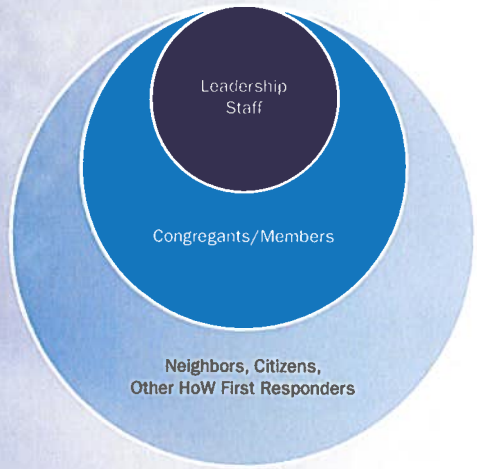


Figure 12. The House of Worship Community

A house of worship should consider all persons who interact with the organization in the security plan.

Best Practices for Your HoW Community

This section focuses on general programs that houses of worship can implement on an individual basis to improve their security posture. HoWs touch many lives and everyone—from clergy, staff, and volunteers, to congregants and visitors—has a role to play, shown in Figure 12.

The overall objective is to create an environment in which your leaders and members are alert to potential threats or problems, aware of the proper channels for reporting, and know what to do in

an emergency. Routine trainings and drills are often the best way to reinforce those lessons—and have saved lives. The following programs and initiatives will help prepare your community for a range of scenarios and is intended for the house of worship as a whole.

Building a Culture of Safety

Houses of worship can improve their security by maintaining an organizational culture based around a shared system of values and goals for safety. An organization's leadership can guide members to embrace these shared values by:

- **Aligning security goals with the organization's core values** and providing consistent messaging about safety and security protocols as a shared community value;
- **Establishing community expectations** related to safety and security and actively facilitating communication, transparency, and responsiveness;
- Implementing a **clear information sharing process** that empowers community members to report incidents and/or concerning behavior, while providing timely feedback after assessing a report and ensuring that confidentiality is maintained;
- **Providing training,** either internally or by leveraging outside sources, such as Cybersecurity and Infrastructure Agency (CISA) Protective Security Advisors (PSAs) and CISA online resources, and offering ongoing learning opportunities on a regular basis;
- **Documenting all security protocols** in written policies and guidelines and ensuring they are shared with the community early and often.

SECURITY IN PRACTICE

PATHWAY TO VIOLENCE

Potential indicators that an individual is on the PATHWAY TO VIOLENCE include:

- **Increasingly erratic, unsafe, or aggressive behaviors**
- **Hostile feelings of injustice or perceived wrongdoing**
- **Harmful use of drugs and alcohol**
- **Marginalization or distancing from friends and colleagues**
- **Changes in work performance**
- **Sudden and dramatic changes in personality and/or home life**
- **Financial difficulties**
- **Pending civil or criminal litigation**
- **Observable grievances with threats or plans for retribution**

Awareness and Early Identification

To meet or alleviate a threat, you must be aware of it. Engaging community members in early identification and reporting is critical. Houses of worship can consider a range of activities and leverage numerous Department of Homeland Security (DHS) resources to empower people with the necessary tools to detect, deter, and mitigate threats:

- **Share the CISA *Pathway to Violence* VIDEO and FACT SHEET with your staff and congregation. DHS has published several resources on understanding the warning signs for an individual who may be on a path to violence.**

- **Familiarize staff with various types of RISK FACTORS AND INDICATORS that could indicate potential violent behavior.**
- **Implement training programs to increase awareness about early warning signs in communications or behavior.**
- **Familiarize yourself with the SUSPICIOUS ACTIVITY REPORTING (SAR) INDICATORS AND EXAMPLES.**
- **Be aware of the conversations within your community, especially when it comes to online activity. Identifying and reporting suspicious activities to the appropriate authorities is crucial for vetting threats for credibility and taking proper mitigation actions.**

If You See Something, Say Something®

Promoting awareness and early identification is one of the most important ways to disrupt a potential threat. The "IF YOU SEE SOMETHING, SAY SOMETHING®" campaign, shown in Figure 13, can help inform your members on how to be alert for suspicious activity and report it through the appropriate channels.

DHS offers a range of products to educate citizens, including a "RECOGNIZE THE SIGNS" infographic and printable POCKET CARD and an "IF YOU SEE SOMETHING, SAY SOMETHING® PUBLIC AWARENESS VIDEO."

Visitors to the "If You See Something, Say Something®" website can also watch a series of videos to "TAKE THE CHALLENGE" and test their powers of observation by spotting suspicious activity.

Figure 13. The "5Ws" of If You See Something, Say Something®

The "5Ws"—who, what, when, where, and why—represent important information to report when contacting local law enforcement or a person of authority.

Image source: https://www.dhs.gov/see-something-say-something

Power of Hello

CISA recommends that houses of worship implement a robust greeter program as a key component of their overall security strategy, centered around the "POWER OF HELLO."

Used effectively, the right words can be a powerful tool. Simply saying "Hello" can prompt a casual conversation with unknown individuals and help you determine why they are visiting your HoW and whether they present a threat. The OHNO approach—**OBSERVE, INITIATE A HELLO, NAVIGATE THE RISK, AND OBTAIN HELP**—helps congregants observe and evaluate suspicious activity and obtain help when necessary:

OBSERVE: Identify suspicious behavior, such as taking pictures/videos of facilities or security features, using abusive language that a reasonable person might find threatening, or loitering at a location without a reasonable explanation.

INITIATE A HELLO: Engage with individuals you observe in your space. Acknowledging a potential threat can act as a deterrent and mitigate risk.

NAVIGATE THE RISK: Ask yourself if the behavior you observe is threatening or suspicious. Is the individual acting in a way that suggests they have a legitimate reason to be there or in a manner that would arouse suspicion in a reasonable person?

OBTAIN HELP: If you believe the individual presents a real threat, do not intervene; obtain help from management or law enforcement. Report your concerns through the appropriate channels at your HoW and always call 9-1-1 for emergencies.

All members of the community have the power to initiate conversations, and to recognize and report suspicious behavior. Sometimes all it takes is a simple "Hello."

SECURITY IN PRACTICE

PRACTICING THE POWER OF HELLO

Smile, make eye contact, and introduce yourself before asking any of the following:

- **"Hello, how are you?"**
- **"May I help you with anything today?"**
- **"How can I assist you?"**
- **"Welcome, is this your first time here?"**
- **"Are you looking for something or someone in particular?"**
- **"Let me take you to the person or place you are looking for."**
- **"I will be here in case you need help."**

Run, Hide, Fight

Sometimes early detection isn't enough to prevent an incident; houses of worship should educate their members on how to respond in the event of an attack. Active assailant situations are unpredictable and evolve quickly. Some active assailant attacks are over before law enforcement arrives on the scene, so individuals must be prepared both mentally and physically to respond to the situation.

- In the event of an armed assailant, such as active shooter, CISA encourages citizens to RUN, HIDE, FIGHT.

Run, Hide, Fight involves quickly assessing the situation and determining the most reasonable way to protect your life given your location and circumstances. In any scenario, you may have one of three options:

1. RUN: If there is an accessible escape path, attempt to evacuate the premises.

- Have an escape route and plan in mind.
- Leave your belongings behind.
- Keep your hands visible and follow any instructions provided by law enforcement.

2. HIDE: If evacuation is not possible, find a place to hide where the attacker is less likely to find you.

- Hide in an area out of the shooter's view.
- Block entry to your hiding place and lock the doors.
- Silence your cell phone (including vibrate mode).
- Remain silent.

3. FIGHT: As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the attacker.

- Act with as much physical aggression as possible.
- Improvise weapons or throw items at the attacker.
- Commit to your actions . . . your life depends on it.

- HoW leaders should share the OPTIONS FOR CONSIDERATION VIDEO with all members of the community to ensure that everyone is familiar with the different options during a potential attack.

SECURITY IN PRACTICE

RUN, HIDE, FIGHT

In over half (n=13) of the total Armed Assault cases (n=20), congregants responded by running or hiding once the attack began. Some were able to escape through exit doors, while others hid in bathrooms, closets, or under furniture. In one case, congregants locked all external doors after hearing commotion outside and prevented the assailant from gaining entry.

In 45 percent (n=9) of the Armed Assault case studies (n=20), members of the congregation or witnesses attempted to tackle, distract, or disarm the perpetrator. Using standard active assailant training, some victims confronted the assailant, a few at the cost of their lives; others threw books, chairs, or furniture. Many of these attempts slowed the assailant enough to allow others to escape to safety.

Mental Health and Social Support Services

Some incidents of targeted violence stem from mental health crises and follow warning signs that a person may be a danger to themselves and others. Not all mental health crises lead to violence; however, HoWs should be aware of signs that an individual is in crisis and may be on the Pathway to Violence.

Houses of worship are uniquely positioned to identify behavioral health concerns and intervene before a situation escalates. HoW leaders are frequently a first point of contact in times of crisis, serving as a sounding board or source of comfort for individuals and families during difficult times. HoWs can promote a culture of caring by enhancing mental health awareness and making it easier for people to seek help. Consider the following options for intervention and assistance to strengthen community resilience:

- **Learn the BASIC FACTS ABOUT MENTAL HEALTH, including possible warning signs that someone needs help.**
- **Educate your community about mental health and foster an open dialogue about mental health and wellness topics.**
- **Identify community members who may be in crisis and connect them with support services.**
- **Develop a system to identify and conduct outreach to members who have not recently attended services.**
- **Review best practices for faith leaders provided through the U.S. Department of Health & Human Services website, MENTALHEALTH.GOV.**
- **Take the ADDRESSING RISK OF VIOLENT BEHAVIOR IN YOUTH online training provided by the U.S. Department of Health & Human Services Substance Abuse and Mental Health Services Administration (SAMHSA).**
- **Identify points of contact that can provide specialized support, such as**

SECURITY IN PRACTICE

DE-ESCALATION

When an armed man dressed in tactical gear threatened church-goers at a Texas church, the pastor intervened and placed himself between the gunman and congregants. Utilizing his experience as a crisis intervention specialist working with troubled youth and offenders, the pastor was able to diffuse the situation by talking to the gunman, who fled and was subsequently arrested the following day.

- **Offer de-escalation training programs for staff, volunteers, and interested members as a potential tool.**
- **Train regularly on lockdown and active shooter procedures.**
- **Educate members and staff on suspicious activity and clearly establish reporting mechanisms.**

mental health, suicide prevention, domestic violence, child abuse, human trafficking, and substance abuse.

- Identify nearby healthcare providers using SAMHSA's tool on FINDTREATMENT.GOV.
- Identify your state's Mental Health Agency using SAMHSA's BEHAVIORAL HEALTH TREATMENT SERVICES LOCATOR.

- **Consider establishing relationships with specialized providers in the community who can serve as a resource for best practices and possible referrals.**

Specialized Policies and Long-Term Planning

Planning is an important stage in the development of a holistic security strategy. Once you've implemented some general best practices, it's time to start planning for a variety of specific scenarios and the potential risks, threats, and outcomes of each. This section highlights some of the more specialized policies for HoW leaders and Security Coordinators to consider as you mature your security program.

Emergency Planning and Incident Response

Planning for emergencies should be a crucial part of any security program and involves determining how your organization will respond to a specific scenario or incident. Emergency Action Plans (EAPs) can help prepare your HoW for any number of emergency situations by providing a roadmap for incident response. CISA has a SUITE OF RESOURCES for incident management planning and response. When creating an EAP, houses of worship can consider the following:

- **Consult the Federal Emergency Management Agency (FEMA) GUIDE FOR DEVELOPING HIGH-QUALITY EMERGENCY OPERATIONS PLANS FOR HOUSES OF WORSHIP (June 2013) for detailed actions that may be taken before, during, and after an incident in order to reduce the impact on property and loss of life. Many HoWs may also benefit from the INCIDENT COMMAND SYSTEM (ICS) training offered by FEMA.**
- **Determine how your HoW will continue to conduct business in any kind of emergency scenario. READY.GOV offers a suite of products in the BUSINESS CONTINUITY PLANNING SUITE that can be adapted to the specific needs of your HoW.**
- **Develop your own EAP using CISA's ACTIVE SHOOTER EMERGENCY ACTION PLAN GUIDE AND TEMPLATE or the CUSTOMIZABLE TEMPLATE PROVIDED BY THE CDC'S CENTER FOR PREPAREDNESS AND RESPONSE.**

These resources cover just a few of the eventualities anticipated by a well-rounded and holistic security strategy. For additional planning resources, see APPENDIX 1.

It is critical that the Safety Team and community members know how to respond if an attack were to occur. The best way to accomplish this is by ensuring community members are well-versed in the EAP and regularly conduct training and drills on emergency procedures.

Personnel Security Practices

Strong personnel security practices can ensure that all staff and volunteers are of good character and maintain standards of integrity and trustworthiness. Houses of worship, like all businesses and organizations, should periodically review personnel security practices to ensure they align with standard business practices and are responsive to evolving threats:

- **Make a list of sensitive positions based on roles and responsibilities.**
  - Are there business operations that require higher levels of scrutiny for personnel supporting those functions?
  - Consider, for example, listing personnel who have contact with children, perform financial tasks, manage and/or maintain personally identifiable information (PII), and have access to information technology (IT) systems.
- **Make a list of positions that should or currently require background investigations and develop and implement policies for automatic employment disqualifiers based on the nature of each position.**
  - Is pre-employment screening conducted for sensitive positions (staff, volunteers, and contractors)? If not, what resources would be required to implement this process?
  - Are periodic self-assessments, formal reviews, and/or background investigation updates conducted for these positions?

Insider Threats

CISA defines an *insider* as any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. Simply put, this is a person the organization and community members trust. An insider threat is the potential for an insider to use their access or special understanding to harm that organization through violence, espionage, sabotage, theft, or cyber means.

Including an insider threat mitigation program as part of a robust security strategy can help increase the number of security-minded employees and community members; reinforce a culture of shared responsibility and asset protection; enable early threat identification; and protect an organization's reputation. CISA recommends that organizations develop their own definition of an insider threat that addresses the unique nature of your HoW, its values, and the resources you feel are most at risk.

An effective INSIDER THREAT mitigation program:

1. **TAILORS THE PROGRAM** to the house of worship's unique mission, culture, critical assets, and threat landscape.
2. **BUILDS A CULTURE OF REPORTING AND PREVENTION**, as outlined in CISA's guidance on how to RECOGNIZE AND REPORT ANOMALOUS BEHAVIOR, that reinforces the positive investment that HoWs make in the well-being of its people, while improving overall resilience and operational effectiveness.

3. **EMPLOYS A LAYERED APPROACH** that considers the variety of roles and functions provided by the HoW.
4. **APPLIES THE FRAMEWORK OF "RECOGNIZE AND REPORT" AND "ASSESS AND RESPOND"** to detect, prevent, and mitigate insider threats (part of the Vulnerability Assessment Process described in Chapter 3).
5. **ESTABLISHES A PROTECTIVE AND SUPPORTIVE CULTURE** to protect civil liberties and maintain confidentiality.
6. **ASSISTS ORGANIZATIONS IN PROVIDING A SAFE, NON-THREATENING ENVIRONMENT** where individuals who might pose a threat are identified and helped before their actions can cause harm.

For more information, refer to CISA's INSIDER THREAT MITIGATION RESOURCES.

Reporting Procedures

Prevention programs and "know the signs" awareness campaigns are most effective when communities know what to do if a potential concern or threat is identified and require deliberate thought on the part of leadership to ensure accountability and clearly define appropriate reporting channels. Houses of worship should clearly outline and communicate reporting standards and mechanisms and ensure all members of the community, especially Safety Team members, are familiar with organizational protocols.

These processes should include reliable and timely evaluation, reporting through appropriate channels, and immediate action in accordance with laws, policies, and regulations. In some cases, reporting might be kept internal and involve the Safety Team or HoW leadership. In other cases, it will be best to report your concerns to law enforcement or federal authorities. To ensure members and staff have the necessary tools to know what, when, and how to report a potential threat, consider the following:

- **Take the Suspicious Activity Reporting (SAR) PRIVATE SECTOR SECURITY TRAINING to better understand how to report suspicious activity and integrate reporting into your organizational culture. Although written for government agencies, 10 WAYS TO INTEGRATE SUSPICIOUS ACTIVITY REPORTING INTO YOUR AGENCY'S OPERATIONS also offers helpful guidance for HoWs.**
- **Familiarize yourself with the NATIONAL SAR INITIATIVE (NSI), which provides a standardized process for identifying and reporting suspicious activity.**
- **Use the "IF YOU SEE SOMETHING, SAY SOMETHING®" campaign and resources to build an internal reporting strategy customized to your organization's culture and security strategy.**
- **Identify individuals within your organization who can serve as trusted contacts for reporting suspicious activity.**
  - › Ensure these individuals are trained in all security protocols.

- Communicate this reporting structure to the community so they know who to contact with security concerns.

- **Establish clear procedures for receiving, assessing, and acting on reports from community members.**
  - Address how to document the notification, handle issues of confidentiality, determine risk probability/impact, notify law enforcement or mental health officials (if appropriate), and conduct further assessment as needed.

- **Circulate the NSI's SAFETY FOR FAITH-BASED EVENTS AND HOWS flier among staff and community members.**

Engaging the Wider Community

Houses of worship play a vital role in community relationships and cohesion, and that role can be a source of strength as you work to improve your HoW's security posture. Some HoWs serve as meeting places for civic groups and support groups, event spaces, entertainment venues, election polling places, and community shelters. Others may strive to make meaningful connections with neighbors and other HoWs in the community.

Engaging your wider community is an important asset for improving overall awareness of potential threats, increasing resilience, and building external partnerships—all of which will strengthen your overall security posture.

Event Planning

While HoWs are designed to be welcoming to non-members, certain types of events can increase risk. Security considerations related to community engagement and event planning should include:

- **Develop and implement event-specific security practices for non-worship activities that take place on the property. Refer to the best practices outlined in the MASS GATHERINGS: SECURITY AWARENESS FOR SOFT TARGETS AND CROWDED PLACES Action Guide for more information.**

- **Identify and continuously evaluate vulnerabilities and potential risks during non-worship activities and enhance security procedures as needed.**

- **Consider whether to incorporate patron screening procedures to prevent prohibited items in facilities during special events and incorporate best practices outlined in the PATRON SCREENING BEST PRACTICES GUIDE and PUBLIC VENUE BAG SEARCH PROCEDURES GUIDE.**

- **Manage visitors and control the number of people in attendance for special events with tickets or sign-up sheets.**

- **Consider reaching out to local law enforcement partners or CISA PSAs to help with security planning for major events such a religious holidays or whenever you anticipate large gatherings.**

Community Engagement

A community-based approach to security includes outreach and awareness activities. As part of a broader security strategy, consider measures that promote community resilience:

- **Engage in public awareness campaigns to educate the community, shape public discourse, and foster understanding, tolerance, and acceptance.**
- **Nominate volunteers and select members of the community for advanced in-person trainings and workshops, such as COMMUNITY EMERGENCY RESPONSE TEAMS (CERT), ACTIVE SHOOTER PREPAREDNESS, Active Assailant, and Hostage Mitigation.**
- **Practice routine, community-wide training exercises and drills with local law enforcement, emergency management, nearby businesses, and other HoWs.**
- **Sponsor and facilitate courses for the community in basic first aid and CPR.**

Faith-based organizations in the community can form partnerships to improve information sharing, enhance resilience, and increase security. Consider creating formal or informal structures and relationships and developing interfaith groups within the community to pool security knowledge and resources:

- **Develop relationships with other HoWs in the same geographical area.**
  - Consider establishing formal, interfaith dialogue groups.
  - Coordinate with the Department of Justice Community Relations Service to organize a PROTECTING PLACES OF WORSHIP FORUM with interfaith community partners.
- **Create a shared, private social media or other communication space for collaboration with other HoWs in your area to centralize information-sharing.**
  - Identify credible threats from peer-to-peer communications, shared information, online activity, and social media, and report to law enforcement as appropriate.
  - Track and report recent threats that emerge online.
- **Coordinate a PREPAREATHON event in your community to encourage community preparation and resilience.**

Strategic Partnerships

Cultivating and maintaining relationships with key community partners and first responders is critical to bolstering your organization's security strategy. Strong community coalitions help further shared goals for identifying threats, mitigating risk, and enhancing public safety. Maintaining an ongoing dialogue with local law enforcement and emergency management services can also improve preparedness and allow for better incident response coordination.

Strategic partnerships can include local police departments, fire departments, and medical emergency services, as well as regional and state organizations. Consider the following steps to foster these important relationships:

- **Identify local partners with first responder oversight for your organization, including:**
  - The local law enforcement agency of jurisdiction;
  - The closest local fire department and emergency medical response unit;
  - The closest hospital trauma center; and
  - Any other nearby medical emergency services, including mental health resources.
- **Establish relationships with local law enforcement and other first responders through regular outreach.**
  - Conduct tours of the property and share building plans to ensure familiarity with the property. Follow up with updated versions if any substantial changes are made to the property and grounds.
  - Review security protocols and conduct and/or participate in formal and informal training sessions.
  - Use community social events to build connections between first responders and the neighborhoods they serve.

SECURITY IN PRACTICE

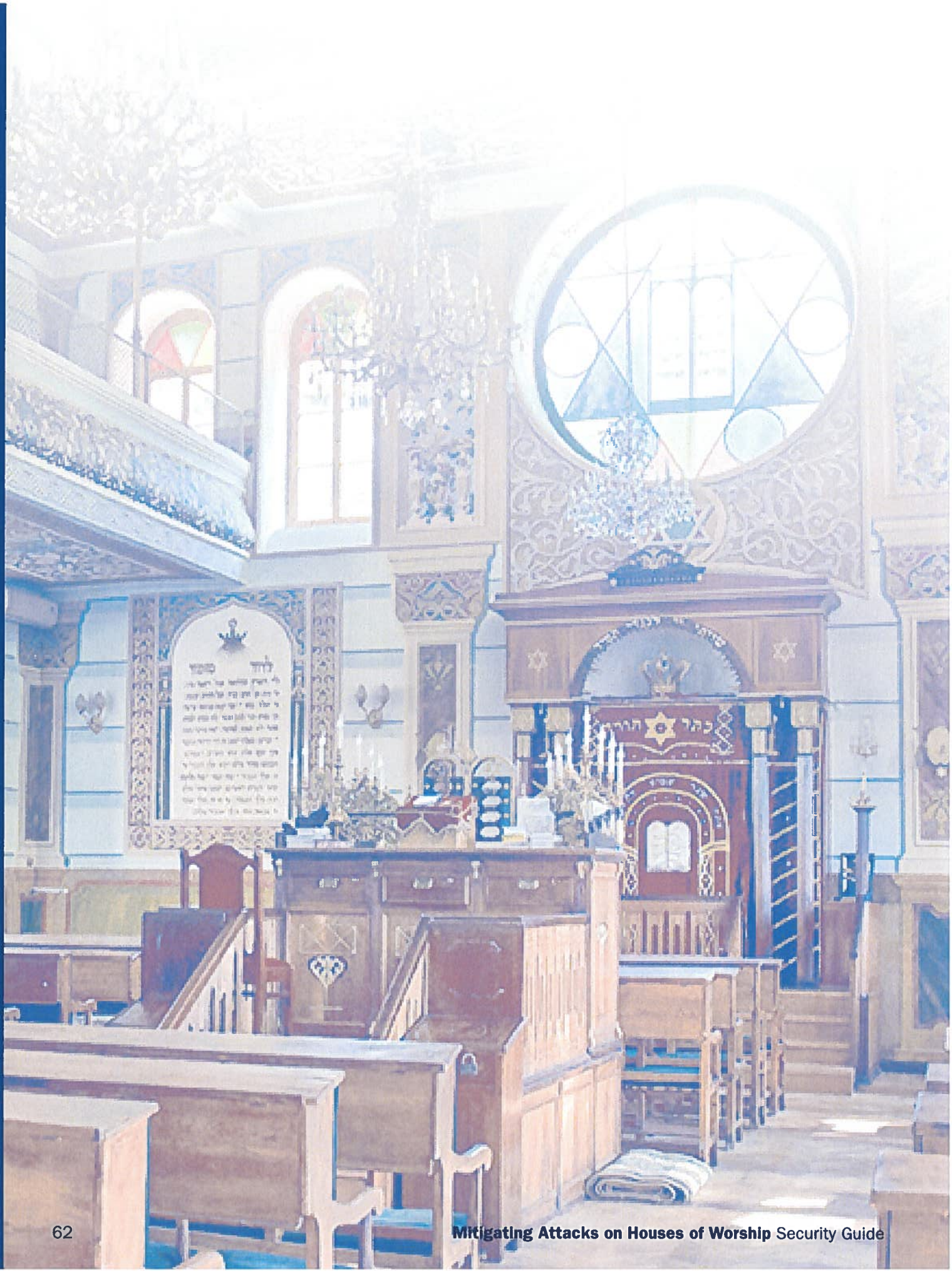
PROFESSIONAL LIAISON PARTNERSHIPS

- **What is the response time to your HoW?**
- **Have they performed a tour of your facility?**
- **Have they responded to your HoW in the past? If yes, for what?**
- **Have they been provided an architectural drawing/floor plans of your facility?**
- **Have they performed training at your HoW? Would they, if invited?**
- **What public safety education and training services can they offer?**

- **Identify your local/regional Emergency Management organization using the READY.GOV TOOL. Reach out to the closest office and subscribe to alerts if offered.**
- **Identify your nearest CISA REGIONAL OFFICE and establish relationships with regional CISA PSAs. View CISA's PSA FACT SHEET for additional information on services provided through this regional program.**
- **If your HoW is located at or within close proximity to a federal facility, connect with the DHS FEDERAL PROTECTIVE SERVICE.**
- **Establish a dialogue with federal law enforcement to learn about planning and training resources and gain a better understanding of suspicious activity reporting and incident response.**
- **Involve your regional fusion center in threat monitoring and investigation.**

Summary

Human behavior, interpersonal relationships, and community values have a huge impact on the effectiveness of security prevention, preparedness, and mitigation programs. HoWs that foster a culture of caring and shared accountability will be well-positioned to respond to current and emerging threats, and the tools presented here can help you find the approach that best fits the needs of your HoW and the wider community it serves.



5 Protecting Your Facilities

Introduction

The intended purpose of any safety and security program is to identify potential risk as early as possible, determine the best plan of action, and minimize or disrupt the risk before it results in bodily harm or property damage. As discussed in Chapter 4, you can address many problems by making changes to the policies, practices, and behaviors within your individual house of worship (HoW)—with minimal capital investment. Yet some vulnerabilities may require physical changes to the structures and grounds of your facility. This chapter outlines some of the options for improvements to physical security, as well as their potential impact.

A welcoming environment does not mean a defenseless one.

To frame the different areas of vulnerability and responsibility, think of your property as divided into three distinct zones: *outer perimeter*, *middle perimeter*, and *inner perimeter*. An effective security strategy must cover the entire responsibility of the HoW, from the outermost reach of the property to the inner most area of the sanctuary. Most security planning begins at the outer perimeter and works inward toward the middle and inner perimeters. Safety features in each zone should be fully integrated and consider interconnected vulnerabilities and risks across zones. This zone system also provides a framework for deploying security programs, like traffic management or greeters.

Mitigation options reviewed in this chapter range from organizing traffic patterns, planting hedges, installing fencing and lighting, closed-circuit television (CCTV) video surveillance, and refining building access controls. Together, these options support a layered approach that encompasses all identified physical security vulnerabilities and risks and considers a range of potential threat scenarios.

The prospect of adding or upgrading physical security can seem daunting, both in terms of cost and the reluctance to "fortify" or "harden" a building that is designed to be open and welcoming. The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes that there are many options available to consider, some of which require minimal capital investment. Many HoWs are also eligible for federal and state grants to offset the cost of improvements, and HoW leaders and security teams can leverage the other freely available resources provided by CISA and other federal agencies outlined in this guide to develop a physical security improvement plan that is tailored to your needs.

GRANT FUNDING

In response to targeted attacks on houses of worship, some state and local governments have passed legislation to create funding opportunities to support security improvements. Be sure to check which could be applicable to your specific HoW.

At the federal level, the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), and Congress are providing increased levels of grant funding to assist HoWs in making security improvements. FEMA offers the NONPROFIT SECURITY GRANT PROGRAM, which provides "funding support opportunities for physical security enhancements and other activities to eligible nonprofit organizations that are at high risk of a terrorist attack and which are located with the geographic footprint of an urban area designated as an Urban Area Security Initiative (UASI) jurisdiction under DHS's UASI Grant Program." Eligible nonprofit organizations may apply to the STATE ADMINISTRATIVE AGENCY. FEMA's Grant Programs Directorate staff are also willing to work with HoWs on emergency preparedness and budgeting guidance to help HoWs plan for security improvements. For more information visit www.fema.gov/grants.

Outer Perimeter

Establishing your HoW's total area of responsibility—the boundary at the outermost edge of the property—is a critical element in the planning process and will be different for every house of worship. The most important aspect is to define this *outer perimeter* in terms of size, existing protection features (e.g., barriers, fencing, gates, and lighting), and observed risks, if any.

The outer perimeter is often the first opportunity to address a vulnerability or mitigate an attack, and every HoW's footprint will present its own unique challenges and circumstances. In some cases, this area may include a large field for sporting events or outdoor activities. In others, the outer perimeter may include a surface parking lot, which may or may not have fencing, lighting, monitoring, or other security features. Some HoWs may have street parking, while others might use multi-story parking facilities that are not affiliated with the organization.

SECURITY IN PRACTICE

SECURITY THROUGH DESIGN

FEMA has issued detailed guidance on how site and building design can help mitigate the risk and damage of an attack.

SITE AND URBAN DESIGN FOR SECURITY: GUIDANCE AGAINST POTENTIAL TERRORIST ATTACKS (2007)
Risk Management Series

REFERENCE MANUAL TO MITIGATE POTENTIAL TERRORIST ATTACKS AGAINST BUILDINGS (2011)
Buildings and Infrastructure Protection Series

Once the Security Planning Team has defined the outer perimeter, it can identify vulnerabilities, determine possible mitigation solutions, and prioritize solutions based on probability, impact, and cost. Houses of worship, particularly those contemplating new construction or renovations, may find useful insights in the concept of Crime Prevention Through Environmental Design (CPTED), which focuses on how the built environment can shape human behavior. Even subtle and cost-effective solutions—such as changes to

landscaping to improve visibility or using concrete planters and bollards to control access—can have significant impact while maximizing return on investment.

One special consideration for the outer perimeter is the threat of vehicular attacks. In general, vehicular attacks fall into two categories: vehicle ramming and vehicle-borne improvised explosive devices (VBIEDs). Both types of vehicle attacks are most likely to occur near the outer perimeter. While the research described in Chapter 1 did not identify any VBIEDs used to target a house of worship, the case studies included two vehicle ramming attacks. Managing traffic patterns and engaging volunteers, greeters, security personnel, or law enforcement to direct traffic, especially during peak times, can help identify suspicious activity. Installing barriers, such as concrete planters or bollards, can also create a "stand-off" zone to help protect congregants.

As you contemplate changes to the outer perimeter, consider some of the following options:

OUTER PERIMETER OPTIONS

Security Features	Types	Benefits & Resources
LIGHTING		
	• Solar Powered • Timed Street Lights	• Deters would-be assailants and/or intruders. • Illuminates all areas so staff and congregants can safely traverse parking lots and grounds.
	Properly maintained lighting features strategically placed along the outer perimeter and throughout the grounds can deter unauthorized access and enhance security for staff and congregants. Options range from solar-powered lighting with night-time illumination to standard streetlights controlled by a timer or on/off switch.	
FENCING/GATES		
	• Visual Barrier • Solid Barrier • Landscape Design	• Limits access to grounds and facilities by individuals not affiliated with the HoW. • Fence style may also offer an aesthetic visual.
	Perimeter fencing and gates feature different styles and functions ranging from simple visual barriers to distinguish property lines to designs that prevent or limit entry onto the grounds. Fences and gates can also be linked to building access control, lighting, and video surveillance systems.	
CCTV (VIDEO SURVEILLANCE)		
	• Record Only • Active Monitoring without Response • Active Monitoring with Response	• Supports monitoring of suspicious behavior and provides early warning capabilities and alerts. • Deters intruders. • Removes blind spots. • PLANNING CONSIDERATIONS: COMPLEX COORDINATED ATTACKS
	Before installing a CCTV surveillance system, consider whether this technology aligns with the overall security strategy, needs, and capacity. CCTV can be implemented in a variety of ways ranging from an unmonitored recording system to a system actively monitored by contracted security and integrated with an incident response plan.	

OUTER PERIMETER OPTIONS

Security Features	Types	Benefits & Resources
TRAFFIC MANAGEMENT		
	• Gates/Bollards • Pathways/Signage • Visitor Parking • Greeters, Volunteers, Law Enforcement	• Defines the flow of people and vehicles. • Supports early warning capabilities and enables non-intrusive visual surveillance. • CISA VEHICLE RAMMING ACTION GUIDE • CISA VBIED DETECTION COURSE FACT SHEET
	A controlled traffic management process safeguards all community members from accidents and vehicular attacks by limiting traffic flow with gates, bollards, traffic cones, signage, or staff directing traffic. Individuals supporting this process should be clearly identified with a reflective vest or uniform. In some circumstances, local law enforcement may be available to assist.	
EMERGENCY COMMUNICATION		
	• Emergency Call-Stanchions (Panic Alert Boxes)	• Abilty to contact HoW security and/or law enforcement in case of emergency. • Minimizes risk in areas away from main buildings in larger facilities.
	Identify areas on the property away from the main building(s) where an emergency call box might be useful, such as a distant parking lot, a walking trail, or prayer garden. Any hardware will require regular maintenance and testing.	
LANDSCAPE		
	• Clear Brush • Install Features	• Improve visibility by removing overgrown brush • Remove any flammable material
	Be sure to maintain the property and grounds. Remove any brush or landscape features that impede visibility or presents a potential hazard. Consider adding landscape features, such as large planters, that may serve to direct traffic or discourage unauthorized access.	

Middle Perimeter

The *middle perimeter* is a fluid area and typically includes anything "on campus" but outside of the main building. For example, walls and exterior doors to the main building would be considered part of the middle perimeter, as would any outbuildings or spaces like playgrounds or picnic areas. Additional buildings, such as a school, rectory, or on-site residence, are considered part of the middle perimeter but require distinct security considerations separate from the main HoW building. Several case studies in Chapter 1 revealed potential vulnerabilities related to middle perimeter security, with attackers moving through or initiating the attack in this zone. Middle perimeter buildings should be described in detail during the vulnerability assessment so that someone unfamiliar with the site—such as a first responder or outside security consultant—can quickly visualize the property and expedite emergency response actions.

The middle perimeter is often where many different kinds of vulnerabilities and threats converge, and it requires a multi-faceted security plan to address these complexities.

Additional considerations for the middle perimeter are picnic areas and/or playgrounds which will be areas of special concern. Often used by children, these spaces should be a top priority for establishing access control features and continuous monitoring, such as with CCTV cameras and/or volunteers and security personnel. If possible, control access to this area through fencing or a physical barrier that would prevent unauthorized entry.

When identifying and prioritizing features to secure the middle perimeter, consider the following options:

MIDDLE PERIMETER OPTIONS

Security Features	Types	Benefits & Resources
DOORS		
	• Wood, Glass, or Metal • Impact or Blast-Resistant	• When locked, secured doors deter intruders and help control crowd flow and access. • Trained greeters strategically situated can help identify suspicious behavior.
	Determine the number of entry points and when they are used. How are they constructed (wood, metal, or glass)? How are they secured (lock and key or access card)? Are they alarmed? Consider if an attacker could block or chain doors to prevent escape during an emergency.	
WINDOWS		
	• Alarmed • Securable with Locks	• When locked, windows deter intruders. • Windows also provide an emergency escape.
	Windows can enable unauthorized entry, especially on the ground level, but also provide an emergency exit if doorways are obstructed. Consider whether they can be locked and secured, but also easily opened if needed? Is there fiber protective material on the glass? Are they alarmed?	
CCTV (VIDEO SURVEILLANCE)		
	• Record Only • Active Monitoring without Response • Active Monitoring with Response	• Supports monitoring and alerts to suspicious behavior, including early warning capabilities. • Deters intruders. • Removes blind spots.
	Areas requiring coverage might include exterior doorway entrances, high-traffic outdoor walkways, or blind spots. CCTV in the middle perimeter can be implemented as unmonitored or monitored with a response plan as previously indicated in the Outer Perimeter CCTV section.	
ACCESS CONTROL		
	• Standard Lock & Key • Electronic Access	• Limits access to authorized individuals and can be aligned with HoW schedules.
	Options include basic lock and key control, more sophisticated electronic applications using access cards or fobs, and software programs integrated with schedules and assigned levels of access.	

MIDDLE PERIMETER OPTIONS

Security Features	Types	Benefits & Resources
INTRUSION ALARMS		
	• Affixed to Doors and Windows	• Rapidly alerts security personnel, law enforcement, or other emergency services to an intruder.
	Consider cost vs. return on investment, organizational security needs, and features that align with the property and facilities, such as motion sensors.	
EMERGENCY GENERATOR		
	• Natural Gas Fueled • Diesel Fueled • Minimum Operation Life: 24 Hours	• Supports emergency services, such as information technology (IT), fire detection, access control, CCTV system, and other connected security features.
	Emergency power generators ensure critical systems are sustained in an emergency, such as lighting for evacuation, elevators, heating, ventilation, and air conditioning (HVAC), and fresh air returns. Power outages can create confusion and distress, which an attacker can leverage to cause more damage and/or injury. Fresh air returns should be above ground level to prevent tampering with the HVAC system. Exposed infrastructure should be covered, protected with locked metal coverings, and monitored by CCTV.	
LANDSCAPING		
	• Clear brush • Install features	• Improve visibilty by removing overgrown brush. • Remove any flammable material.
	Be sure to maintain the property and grounds. Remove any brush or landscape features that impede visibility or presents a potential hazard. Consider adding landscape features, such as large planters, that may serve to direct traffic or discourage unauthorized access.	

Inner Perimeter

The sanctum, or *inner perimeter*, will undoubtedly be the most important area to protect because this is where your most important asset will be located: your people. In most cases, this will be the main building, but additional structures, such as schools, rectories, or residences, will have their own inner perimeters that may include children's rooms, administrative offices, prayer rooms, or other common areas.

Of the 37 acts of targeted violence examined in Chapter 1, 43 percent (n=16) took place within the inner perimeter or sanctum. As the site where people often gather in the greatest numbers, attacks within the inner perimeter often represent the greatest loss of life. To protect your people, the inner perimeter zone requires the highest level of scrutiny, control, and monitoring.

Security measures focused on the inner perimeter should be as detailed as possible. Members of the Safety Team should have clearly defined roles and responsibilities. All congregation members should be aware of the basic security trainings identified in Chapter 4 and understand the protocols for emergency evacuation or active assailant scenarios. For special considerations related to security measures for school and daycare facilities, see Chapter 6.

Inner perimeter security generally includes the following:

INNER PERIMETER OPTIONS

Security Features	Types	Benefits and Resources

SANCTUARY

- Main Area of Worship
- Largest Congregation of People
- Active Shooter Preparedness Program

- Training of Congregants on Emergency Procedures
- CISA ACTIVE SHOOTER PREPAREDNESS

The sanctuary is one of the most important areas to protect and should be a main focus of the security planning process. Incident management and emergency action plans should center around the sanctuary and the services performed there.

RECEPTION/VISITOR MANAGEMENT

- People are a HoW's Greatest Safety Asset
- Power of Hello
- Identify Suspicious Activity Training

- Enables rapid identification of suspicious activity, mail, or phone calls.
- Helps control flow of HoW visitors and manage access.
- CISA POWER OF HELLO RESOURCES

Consider implementing a visitor management system. For HoWs with administrative or reception staff, provide appropriate training and implement detailed security procedures, including a list of authorized/pre-screened visitors, notification and screening, handling suspicious mail/phone calls, and reporting suspicious activity. Be sure all visitors are aware of emergency exits.

ACCESS CONTROL

- Standard Lock & Key
- Electronic Access

- Limits access to authorized individuals can can be aligned with HoW schedules.

Options include basic lock and key control, more sophisticated electronic applications using access cards or fobs, and software programs integrated with schedules and assigned levels of access.

CHILDREN'S ROOMS/SCHOOL

Refer to Chapter 6

SHELTER-IN-PLACE ROOM

- Windowless room with doors that lock or other secure interior space

- Provides a safe room to hide during an active shooter incident
- REFERENCE MANUAL TO MITIGATE POTENTIAL TERRORIST ATTACKS AGAINST BUILDINGS
- RISK ASSESSMENT: A HOW-TO GUIDE TO MITIGATE POTENTIAL TERRORIST ATTACKS AGAINST BUILDINGS

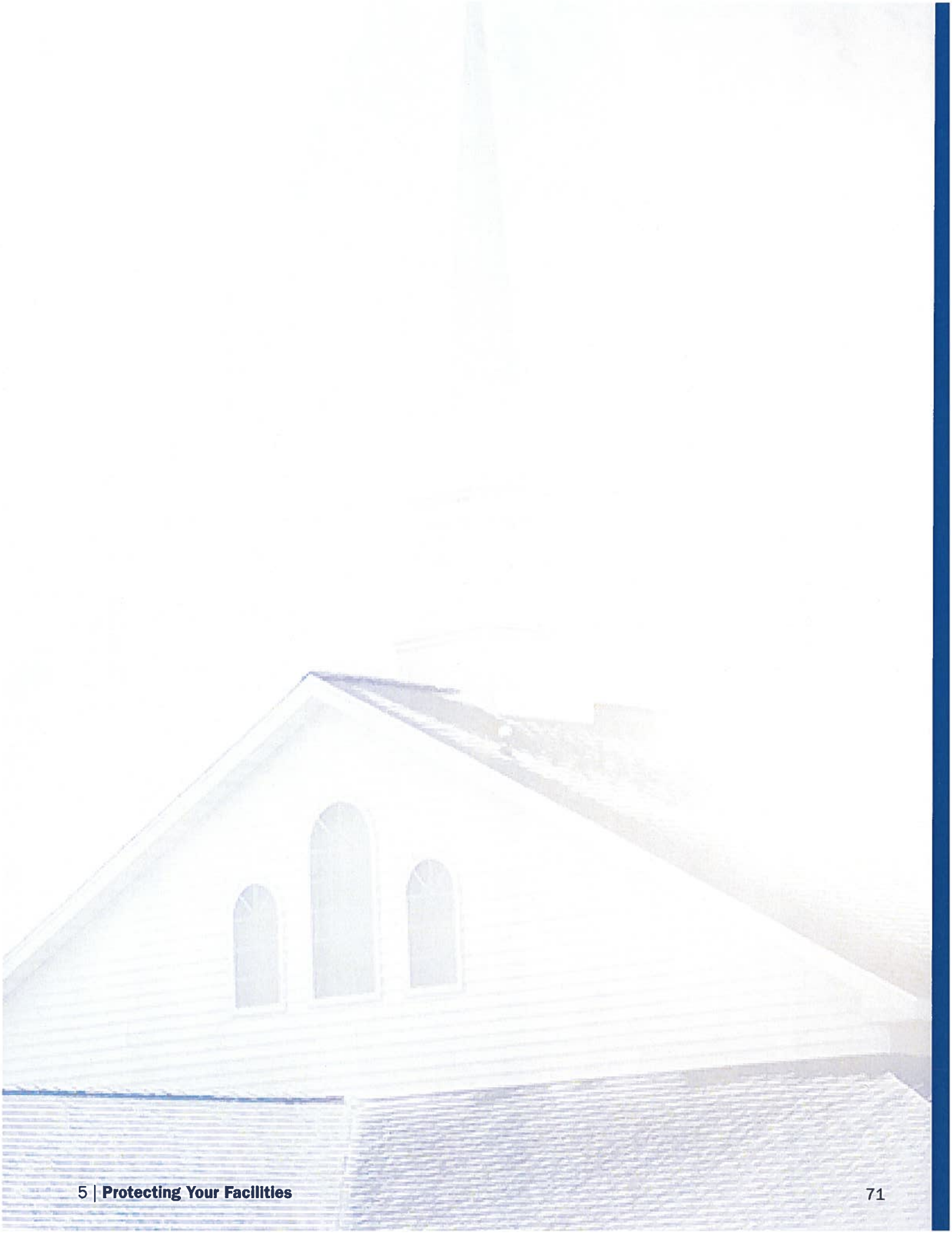
Identify shelter-in-place or "safe rooms" for use during severe weather and/or during an incident, such as an active shooter. These locations should be rooms without windows and with doors that lock. Staff and visitors should know the location and understand the purpose of these rooms. Training can help prepare staff to guide members to these locations in an emergency. Shelter-in-place plans should address severe weather scenarios, such as tornados or hazardous material incidents where breathing outside air could pose a threat.

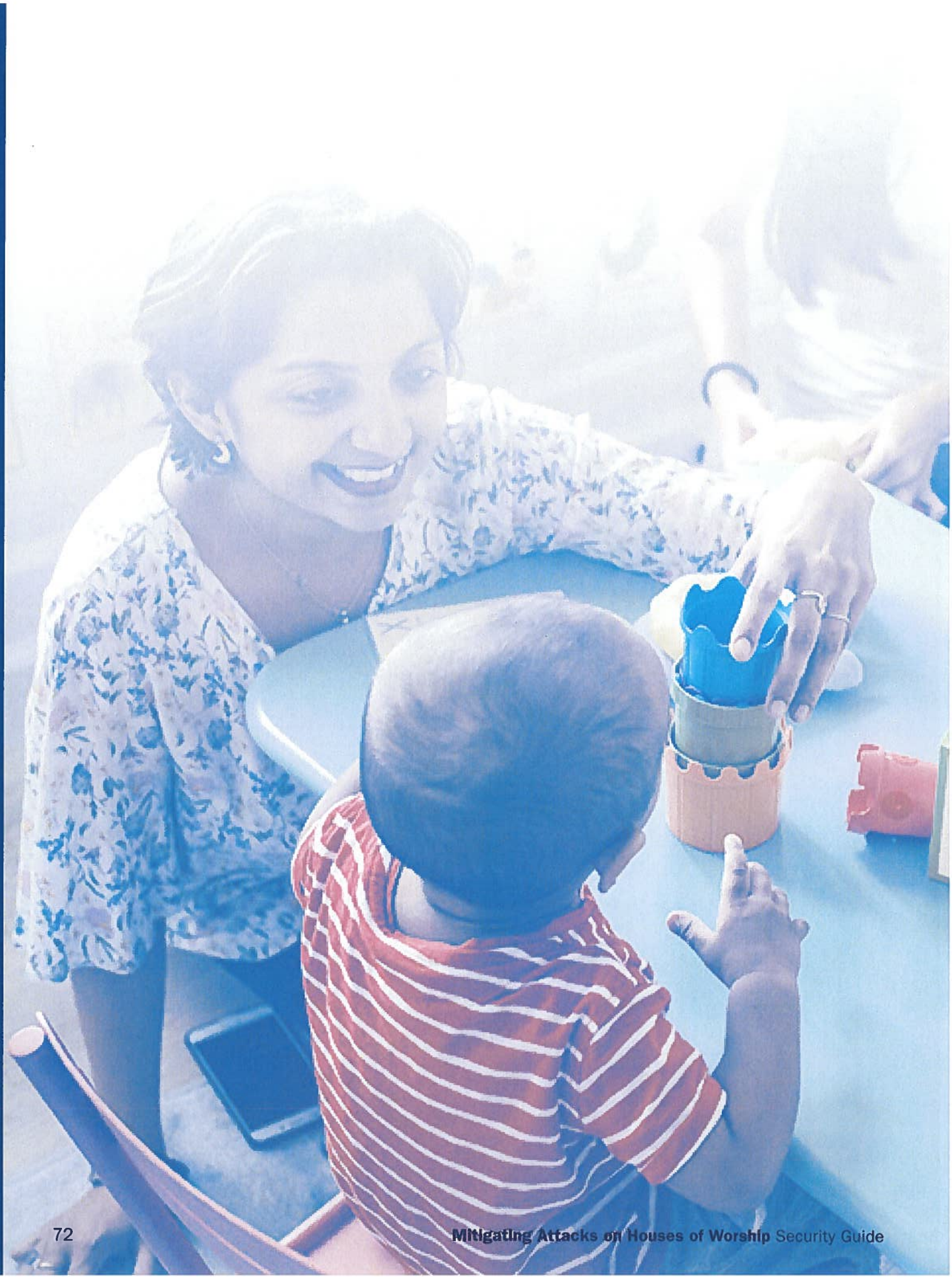
INNER PERIMETER OPTIONS

Security Features	Types	Benefits and Resources
FIRST AID/AED		
	• Store bought • Professionally serviced	• Staff and congregants have the necessary tools to respond quickly in an emergency. • YOU ARE THE HELP UNTIL HELP ARRIVES
	Life-saving equipment, such as first aid kits and automated external defibrillators (AEDs), should be kept in clearly marked locations and regularly checked to ensure supplies are fully stocked and unexpired. AEDs should be tested and maintained for proper functionality. Supply companies can be contracted to provide this service.	
FIRE ALARM AND SUPPRESSION SYSTEMS		
	• Store bought • Professionally serviced	• Rapidly alerts security personnel, fire department, or other emergency services in a fire emergency.
	Fire and smoke alarms, along with fire suppression systems, should comply with state, county, and municipal standards. Most buildings undergo inspections for emergency systems prior to receiving an occupancy permit. Every HoW should have functional and compliant smoke and fire detectors. These alarms should be inspected annually to ensure they are fully operational. Fire extinguishers should be positioned throughout all buildings and well-marked for easy access in an emergency. These should also be checked and maintained as required by local standards.	

Summary

Dividing the area of your house of worship's responsibility into an outer, middle, and inner perimeter offers a useful framework for organizing your security programs and contemplating the upgrades or modifications that might be necessary to improve physical security. Your vulnerability assessment will help facilitate the process of identifying vulnerabilities and risks and prioritizing any changes you deem necessary in the most efficient and cost-effective manner possible.





6 Daycare and School Safety Considerations

Introduction

Providing children with a safe space to learn and develop is a core value in communities nationwide. Schools and daycares are particularly vulnerable to targeted violence, leading many to implement robust security programs in recent years. The threat of school violence is further magnified for K-12 schools, summer programs, daycare facilities, religious study and after school programs, and weekend care programs affiliated with houses of worship. Ensuring safe environments for children and educators is essential and houses of worship (HoWs) should prioritize security planning for school or daycare facilities while considering the full scope of associated vulnerabilities and risks. The guidance offered here is based on the FOUNDATIONAL ELEMENTS of school safety as developed by the Department of Homeland Security (DHS) and detailed at SchoolSafety.gov.

Assess the Facilities

Begin by assessing the site and needs of the community affiliated with the school or daycare facility, such as the number of students and faculty, number of exits and entrances, and number of rooms. This will support a more accurate assessment and security plans that are tailored to effectively safeguard these facilities. To streamline this process, the Cybersecurity and Infrastructure Security Agency (CISA) recommends using no-cost assessments, including that of CISA's K-12 GUIDE AND ASSESSMENT TOOL, or the READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS (REMS) SITE ASSESS APP administered by the U.S. Department of Education.

SchoolSafety.gov provides education facilities with the tools to maintain a safe environment for children and educators. Resources are organized across the preparedness continuum: **PREVENT, PROTECT AND MITIGATE, RESPOND AND RECOVER**. School and daycare center staff can take a self-assessment to receive a personalized action plan with next steps and access a range of valuable resources, trainings, and aligned grant funding.

No one-size-fits-all approach exists for childcare and education. However, many resources are available from the government and the private sector to help HoWs develop and implement security measures for schools and daycares in accordance with local statutes. These include resources about school security policies, physical security, school climate, behavioral health techniques, training, and funding opportunities. CISA Protective Security Advisors (PSAs) are also available to provide professional on-site assessments.

Procedures and Protocols

The right set of procedures and protocols is essential to preventing and responding to threats. Consider establishing a School Safety Action Plan and EMERGENCY OPERATIONS PLAN (EOP), and assign security roles to specific staff to prepare for a range of threats to a school or daycare facility. Security measures should address both physical and behavioral security considerations, as well as institutional policies. A thorough planning process should include the following steps:

- **Create a personalized SCHOOL SAFETY ACTION PLAN to identify important next steps to help secure your school.**
- **Analyze vulnerabilities across current policies, such as missing information, lack of guidance, and/or outdated practices, and cross-reference this list against best practices to identify areas where new procedures or improvements may be needed.**
- **Take the online course DEVELOPING EMERGENCY OPERATIONS PLANS (EOPs) K-12 101 to learn more about creating an effective EOP and implementation plan.**
- **Use the interagency GUIDE FOR DEVELOPING HIGH-QUALITY SCHOOL EMERGENCY OPERATIONS PLANS to establish foundational principles and follow the six-step planning process.**
- **Employ DHS's RECOVERY STRATEGIES and resource list to facilitate the creation of a robust recovery plan.**

Key policies to consider incorporating into security plans include:

- **Policies for child pick-up and drop-off**
- **Policies for child guardians or persons with legal responsibility over a child, aside from a parent**
- **Policies for supervising recess and implementing adequate physical security measures**
- **Protocols for domestic disputes**
- **Protocols for visitors and suspicious persons on or around the property**
- **Protocols for an active incident in another building on the property**

Physical Security

Physical security considerations for schools and daycares include added vulnerabilities, such as playgrounds, classrooms, and designated drop-off/pick-up areas. Houses of worship should align physical security planning with the broader recommendations provided in Chapter 5 and tailored to the risks associated with these unique elements. HoWs should consider the following additional precautions:

- **Assess the current physical security posture of the school/daycare with the help of a CISA PSA, SchoolSafety.gov resources, or by using the DHS SCHOOL SECURITY SURVEY to identify gaps in physical features and equipment, and prioritize updates.**
- **Use the Readiness and Emergency Management for Schools (REMS) SITE ASSESS SECURE MOBILE APP to conduct a security assessment and receive a customized to-do list.**
- **Implement security enhancements within the various perimeters, as outlined in PARTNER ALLIANCE FOR SAFER SCHOOLS – SAFETY AND SECURITY GUIDELINES FOR K-12 SCHOOLS.**
- **Consider PHYSICAL SECURITY STRATEGIES recommended by SchoolSafety.gov.**

School Climate

Providing students with a range of social, emotional, and behavioral support systems can build strong character skills and allow students to connect with their peers and educators in more meaningful ways. These systems can improve school climate and prevent violence, while supporting mental health and empowering students to speak up when something seems suspicious or dangerous. A 2019 U.S. Secret Service (USSS) report found that 80 percent of school attackers previously exhibited behavior that caused concern for both public safety and the attacker's safety.[1] Providing HoW staff and students with a safe environment that encourages everyone to report concerning behaviors helps decrease the likelihood of violence through early intervention. For this approach to be successful, schools must not only prioritize school climate but also provide guidance on available reporting mechanisms. HoWs can refer to the following resources to improve overall school climate within affiliated schools and daycares:

- **Review GUIDING PRINCIPLES: GUIDE FOR IMPROVING SCHOOL CLIMATE to learn about three critical principles for fostering a positive school climate.**
- **Use the SCHOOL CLIMATE IMPROVEMENT ACTION GUIDES to assess five key actions for enhancing school climate. Each step will provide action items, do's and don'ts, and questions for consideration.**
- **Visit SCHOOL CLIMATE resources on SchoolSafety.gov to access additional topical resources and available grant options.**

1 National Threat Assessment Center, *Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence* (2019), U.S. Secret Service, U.S. Department of Homeland Security, https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf.

Behavioral Health

Promoting behavioral health for students—as well as faculty and staff as described in Chapter 4—is an important step toward preventing violence in schools. Students struggling with mental and behavioral health challenges often also see impacts to their social and academic success. For example, a 2017 survey found that approximately 20 percent of students from 12–18 years have experienced bullying.[2] Bullying is a common occurrence that can severely impact physical and mental health and has been a factor in some cases of school violence. By using available resources to help identify concerning behaviors and implementing efforts to improve students' mental and physical health, HoWs can help create safer environments in their schools and daycare centers.[3] Consider the following steps and resources to identify and address threatening or concerning behaviors before they can lead to violence:

- **Conduct a behavioral threat assessment to evaluate potential suspicious activity and enhance behavioral health support.**
  - A dedicated multi-disciplinary team including and supported by qualified professionals from a variety of disciplines should conduct this assessment. The team should include at minimum a school administrator, a mental health counselor, and a school resource officer.
  - Once training is complete and clear roles are established, the team should create comprehensive written plans, policies, and procedures for the behavioral threat assessment process, including a process to evaluate reported threats and concerning behaviors.
  - The team should continually review reported threats and other concerning behaviors to identify areas for intervention and mitigation.
  - Detailed guidance and resources for creating teams, conducting threat assessments, and creating subsequent policies and procedures for schools can be found using the USSS ENHANCING SCHOOL SAFETY USING A THREAT ASSESSMENT MODEL.
- **Complete the SCHOOL HEALTH ASSESSMENT AND PERFORMANCE EVALUATION SYSTEM's School Mental Health Profile to produce an overview of existing mental health services and systems. This overview will help identify gaps and contribute to national-level tracking for mental health systems in schools.**
- **Conduct the BULLYING PREVENTION CAPACITY ASSESSMENT AND CHANGE PACKAGE to determine your school's capacity to prevent bullying in seven areas.**
  - Following the assessment, utilize the Bullying Prevention Portfolio to review evidence-based drivers for bullying prevention to enhance current capabilities.

2 "Facts About Bullying." StopBullying.gov, U.S. Department of Health and Human Services, August 12, 2020, https://www.stopbullying.gov/resources/facts#stats.

3 "Bullying and Cyberbulling," SchoolSafety.gov, U.S. Department of Homeland Security, https://www.schoolsafety.gov/prevent/bullying-and-cyberbullying.

Training

Training, exercises, and drills are essential to an environment in which school and daycare staff can help prevent and respond to emergency situations. Students should be trained on best practices for remaining safe during incidents such as hazardous weather or active shooters. Understanding policies, roles, and procedures helps to streamline response efforts and mitigate the risk of negative outcomes. HoWs can consider the following strategies for training school staff and ensuring policies, processes, and procedures remain current:

1. Train school administrators and staff on all aspects of the school's EOP and implementation plan with the following steps:
    A. Train staff on roles and responsibilities within the EOP.
    B. Designate a staff member to coordinate and execute EOP exercises.
    C. Conduct annual exercises with all staff to practice EOP procedures. Include community partners where appropriate.
    D. Evaluate current plans while conducting training exercises to update the EOP accordingly.[4]
2. Submit an application for REMS TRAINING BY REQUEST to receive free in-person training on developing EOPs and resilience strategies.
3. Complete self-conducted table-top exercises for students and faculty members using DHS CAMPUS RESILIENCE PROGRAM EXERCISE STARTER KITS.
4. Employ principles from the HOMELAND SECURITY EXERCISE AND EVALUATION PROGRAM GUIDELINES to develop, execute, and evaluate additional exercise programs. The guide should be used in accordance with organizational priorities for school safety initiatives and policies.
5. Review the TRAINING, EXERCISES, AND DRILLS offered on SchoolSafety.gov for additional strategies and resources.

4 "Training, Exercises, and Drills." SchoolSafety.gov, U.S. Department of Homeland Security, https://www.schoolsafety.gov/respond-and-recover/training-exercises-and-drills

Funding Resources

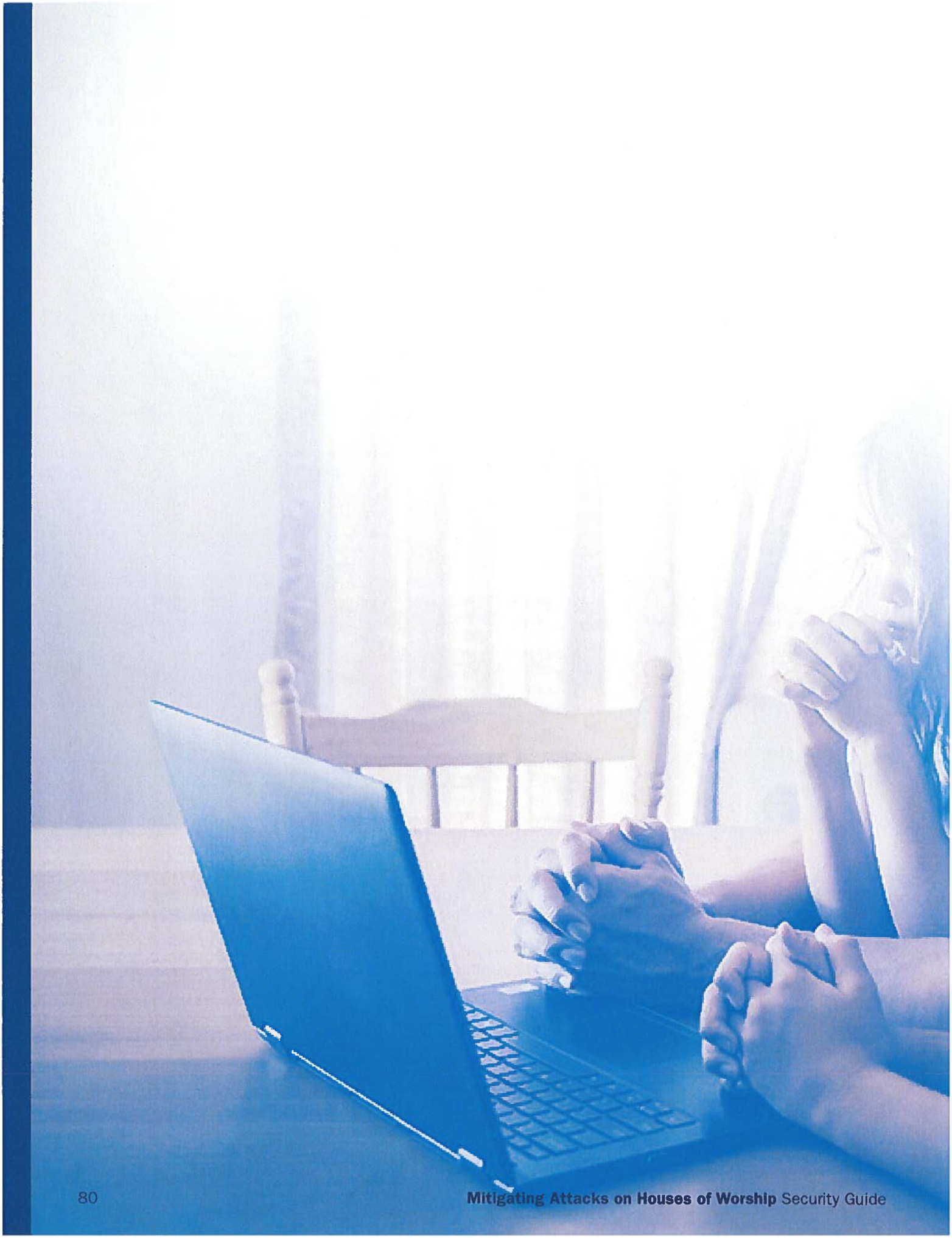
Non-profit HoW schools may be eligible to receive the grants outlined below following an application to either their State Awarding Agency (SAA) or directly from the awarding entity:

- **NONPROFIT SECURITY GRANT PROGRAM**
  - Supports security enhancements for nonprofit organizations with a high risk of a terrorist attack.
- **SCHOOL VIOLENCE PREVENTION PROGRAM (SVPP)**
  - Helps improve security for schools in the grantee's jurisdiction through evidence-based school safety programs.
- **STOP SCHOOL VIOLENCE TECHNOLOGY AND THREAT ASSESSMENT SOLUTIONS FOR SAFER SCHOOLS PROGRAM**
  - Enhances efforts to reduce violent crime by creating school threat assessment teams, using technology for anonymously reporting suspicious activity related to violence in schools, and by creating and enhancing State School Safety Centers.
- **PROJECT SCHOOL EMERGENCY RESPONSE TO VIOLENCE (SERV)**
  - Funds short-term and long-term education-related services for local educational agencies (LEA) and institutions of higher education (IHE) to support recovery following a violent or traumatic event that has disrupted the learning environment.
- **E-RATE PROGRAM**
  - Gives public schools and libraries cost-effective access to technologies that bolster network infrastructures and prepare for future educational requirements.

For additional grants opportunities, visit SchoolSafety.gov.

Summary

Schools and daycares affiliated with houses of worship share many of the same characteristics and vulnerabilities as similar facilities around the country, with an added layer of risk due to faith-based affiliations. HoWs with such facilities should maintain constant awareness of these unique challenges and threats when developing and implementing robust security policies to protect students and teachers and safeguard their learning environment.



7 Cybersecurity

Introduction

The Internet has allowed faith-based communities to connect in unprecedented ways. Many houses of worship (HoWs) take advantage of technologies like live-streaming services and building community through online portals. This connectivity allows for great access, but it also opens the door to new and emerging threats. Cyber actors are constantly looking for new targets and vulnerabilities to exploit and HoWs are not immune.

Faith-based organizations are vulnerable to cyberattacks due to the types of information they access and store; they are seen as easy targets due to their size and perceived lack of cyber protections. As part of standard business operations, faith-based organizations collect and store large amounts of personal and financial information from congregants, donors, and employees. Such personally identifiable information (PII) can be used to commit identity theft, to steal from bank accounts, and to identify targets for additional exploitation. In addition to cyber actors motivated by financial gain, perpetrators may target HoWs for ideological reasons. In either case, a cyberattack can hurt the reputation of a HoW in ways that are difficult to overcome, possibly interfering with the institution's overall mission.

Cybersecurity should be treated as an extension of other security and contingency plans.

Types of Cyber Attacks

While malicious cyber actors can employ various methods, the incident analysis conducted for this report revealed that HoWs are particularly vulnerable to the following types of attacks:

Financial Exploitation

Much like any organization that handles money, HoWs are at risk of financial exploitation. Many faith-based organizations now collect donations using online or mobile platforms, creating new vulnerabilities and opportunities for exploitation. Financial exploitation can be tied to a variety of nefarious methods, including network intrusions that result from phishing and malware.

Ransomware

An increasing number of malicious cyber actors use ransomware—a type of software designed to deny access to a computer system or data until a fee is paid—to attack soft targets like hospitals and municipal governments. In these types of attacks, cyber actors gain access to vulnerable networks and encrypt files before demanding payment.

Website Defacement

Another potential vulnerability comes in the form of website defacement, wherein a cyber actor gains entry to a network or web server and changes or replaces the website content with their own information. These attacks, which typically feature hateful language or imagery, seek to cause fear and undermine a community's efforts to create interfaith dialogue. Faith-based communities are increasingly victimized by website defacement attacks.

Creating a Culture of Cyber Readiness

Reducing cyber risk requires a holistic and multi-layered approach, much like the approach used to address physical threats. HoWs must incorporate cyber resiliency into any security plan that addresses institutional and congregant preparedness. Managing cyber risk requires HoWs to build strong security practices and a *culture of cyber readiness* by encouraging basic cyber hygiene and data protection throughout the organization.

As the Nation's risk advisor and lead civilian agency charged with safeguarding the Nation's cyberspace, the Cybersecurity and Infrastructure Agency (CISA) is responsible for building national capacity to defend against cyberattacks. CISA is dedicated to developing and providing faith-based communities with a range of resources aimed at empowering HoWs to mitigate a range of cyber threats. HoWs of all sizes can use the resources and tips outlined below to begin making changes for a safer and more secure online presence.

CISA offers direct cybersecurity expertise and recommends developing relationships with regional CISA CYBER SECURITY ADVISORS (CSAs) to bolster cybersecurity preparedness, risk mitigation, and incident response capabilities.

SECURITY IN PRACTICE

CREATING A CULTURE OF CYBER READINESS

6 Essential Elements of a Culture of Cyber Readiness

Yourself	Drive cybersecurity strategy, investment, and culture
Your Staff	Develop security awareness and vigilance
Your Systems	Protect critical assets and applications
Your Surroundings	Ensure only those who belong on your digital workplace have access
Your Data	Make backups and avoid the loss of information critical to operations
Your Actions Under Stress	Limit damage and quicken restoration of normal operations

For more, see: CISA'S CYBER ESSENTIALS

CISA CYBERSECURITY ADVISORS (CSAs)

WHO?	Regional CISA personnel who offer assistance and front-line support to help prepare and protect stakeholders from cybersecurity threats.
WHERE?	Distributed across the ten CISA regions throughout the United States.
WHAT?	Engage private sector entities and state, local, tribal, and territorial (SLTT) governments through partnerships and direct assistance activities, such as on-site meetings, working group facilitation, and incident coordination and support.
WHY?	Promote cybersecurity preparedness, risk mitigation, and incident response capabilities, and create channels of communication between the public and the Department of Homeland Security (DHS) cyber programs.

Cyber Hygiene

Organizations must build a culture of cyber readiness from the ground up, which may require a shift in thinking. Cyber hygiene entails implementing basic levels of cybersecurity and improving general awareness of risk among staff, volunteers, and congregants to improve resilience and mitigate the effects of a potential intrusion or attack. Cybersecurity is increasingly important as our culture continues to depend on cyber technology and the benefits it offers and is an important consideration for organizations of all sizes and locations.

HoWs should prioritize awareness of key cybersecurity concepts and adopt industry best practices, and most internet service providers stand ready to help address many common vulnerabilities. In addition to the steps outlined in the CYBERSECURITY RESOURCES ROADMAP, there are several common-sense approaches that faith-based organizations can use to build a culture of cybersecurity:

- **Refer to CISA's CYBER ESSENTIALS for key information regarding organizational cyber readiness.**
- **Stay current on security updates and enable automatic updates whenever possible.**
  - UNDERSTANDING PATCHES AND SOFTWARE UPDATES
- **Subscribe to the NATIONAL CYBER AWARENESS SYSTEM (NCAS) to receive cybersecurity alerts, analysis reports, bulletins, or tips.**
- **Regularly back up important files and data.**
  - Important files that need additional back up and protection might include: financial records; congregant lists, addresses, and PII; property records; employee and volunteer files; online donation records, etc.

- **Maintain awareness of suspicious emails and exercise caution when opening attachments or links (USING CAUTION WITH EMAIL ATTACHMENTS).**
- **If available, enable two-factor authentication (2FA) on website administrator accounts.**
- **Understand RISKS TO MOBILE PHONES and make adjustments to secure mobile devices affiliated with your HoW.**
- **Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Apply these polices consistently.**
- **Establish rules of behavior for handling and protecting congregant and donor information and other vital data. Consider restricting access or password protecting files and installing software to protect the website and donations platform.**
- **Install anti-virus software on all computers and update regularly.**

Online Safety

The Internet makes it easier for faith-based organizations to connect with both members and potential new members while social media provides an effective way to stay connected and share updates. However, ease of access and informality also make these platforms attractive to malicious actors who may exploit information that is readily available. While many sites are benign, social media platforms have been used to distribute malicious code. Similarly, personal information posted on social media can be used to conduct social engineering attacks or used in preparation for physical attacks, such as the exploitation of worship schedules or plans. Even without sophisticated technological actors, online platforms are exploited by those seeking to bully or intimidate.

SECURITY IN PRACTICE

CHOOSING SECURE PASSWORDS

DO:	DON'T:
• Use the longest password allowed	• Use words that can be found in the dictionary
• Use symbols and numbers	• Use passwords based on personal information
• Use different passwords for each account	• Share your password

Adopting basic levels of security and awareness can allow HoWs to continue safely connecting online. The following resources can help you safely connect online:

- **Implement general online privacy best practices, as outlined in the ONLINE PRIVACY TIP SHEET.**
- **Review STAYING SAFE ON SOCIAL NETWORKING SITES and the SOCIAL MEDIA CYBERSECURITY TIP SHEET to understand the range of threats associated with social media.**
- **Refer to the GUIDELINES FOR PUBLISHING INFORMATION ONLINE and monitor the information posted on facility websites or social media accounts, including worship and activity schedules. Consider posting schedules weekly, rather than monthly, or restricting schedules to a member portal.**
- **Be mindful of what is being emailed to the congregation. Keep distribution lists up to date to ensure you are only emailing current members with a need for the information.**
- **Make adjustments to prioritize socializing securely.**
- **Cyberbullying can range in severity and may indicate a tendency toward more serious behavior. Understand the basics of cyberbullying and refer to DEALING WITH CYBERBULLIES for information on protecting your community.**
- **Understand the risks posed by social engineering and implement the procedures outlined in AVOIDING SOCIAL ENGINEERING AND PHISHING ATTACKS.**

Security Practices and Awareness

In addition to basic best practices that all individuals and organizations may adopt, HoWs may consider implementing more advanced measures to improve resilience against potential cyber incidents. A robust cybersecurity program will include activities that focus on cyber incident response planning, educating key stakeholders, and developing reporting protocols to identify suspicious activities. Building an effective cybersecurity program requires both an awareness of tactics and a new way of thinking. HoWs should consider the following:

- **Identify thresholds and methods for reporting cyber incidents—both internally to the security program manager and externally to authorities—by referring to the HOW TO RECOGNIZE AND PREVENT CYBERCRIME tip card and CISA's site for REPORTING CYBER INCIDENTS.**
- **Talk to other faith-based institutions about what they are doing to protect themselves. Be sure to share what information you have in order to help them as well.**
- **Subscribe to the US-CERT MONTHLY BULLETIN for information regarding cybersecurity webinars and workshops, new publications, and best practices.**
- **Conduct a self-led CISA CYBER RESILIENCE REVIEW (CRR) to measure existing security measures and identify areas for improvement.**
- **Know how to communicate and who to involve during a crisis, including REPORTING CYBERATTACKS AND INCIDENTS TO CISA and the appropriate authorities.**

- **Create a detailed inventory list of data and physical assets and update it routinely.**
  - Include the manufacturer, model, serial number and support information for hardware and software. For software, include the specific version that is installed and running.
  - Know where data and technology are stored and who has access to both.
- **Conduct vulnerability tests on your website by either using a paid vulnerability scanning service or CISA's free static internet protocol (IP) scanning to detect known exploits and weaknesses.**
- **Refer to CISA INSIGHTS: REMEDIATE VULNERABILITIES FOR INTERNET-ACCESSIBLE SYSTEMS for more information. Make regular backups of data to avoid loss of information critical to operations.**
  - Consider a range of data backup options that may include employing a backup solution that automatically backs up your data.
  - Maintain both online and offline backups that are not permanently connected to the computers and networks that they are backing up. This practice reduces the risk of a damaged backup.
- **Define expected behavior across the organization to create a culture of security among staff. Require adherence to end-user agreements and enterprise cybersecurity policies.**
- **Build a network of trusted relationships with faith-based partners and local government agencies for threat sharing and access to timely cyber threat information.**
- **Attend a CISA-led regional meeting focused on evolving cyber risk management needs and community resources available to various sectors and regions.**
- **Use CISA's scalable CYBER TABLETOP EXERCISE PACKAGE (CTEP) to produce and customize a tabletop cyber exercise tailored for your organization.**
- **Organizations should determine their risk of DISCLOSING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION. Once this risk is determined, they should follow industry best practices to prevent its disclosure.**
- **Develop and train staff on a comprehensive cyber incident response plan that focuses on being able to recover systems, networks, and data from known, accurate backups.**
  - Ensure that this plan is formally approved by your organization's senior leadership to ensure its acceptance.
  - Regularly test your incident response plan to ensure that each part of your organization knows how to respond to both basic and large-scale cybersecurity incidents.

Combatting Specific Threats

Cyberattacks come in a wide variety of forms and each requires a specific response. Fortunately, these countermeasures often overlap and are a vital part of creating a robust culture of cyber hygiene and readiness.

Malware and Viruses

Malware and viruses are malicious software programs designed to compromise the integrity of your computer or mobile device and give attackers the ability to monitor your activity or steal your data. There are several important considerations for protecting yourself and your organization against malware and network intrusions:

- **Educate your staff on the different types of malware that can infect devices and the best practices for protecting such devices. Read the CISA MALWARE TIP CARD.**
- **Keep all security software, web browsers, and operating systems up to date to prevent attackers from taking advantage of known vulnerabilities.**
- **Avoid clicking on suspicious links in emails or online posts.**
- **Use security software to scan universal serial bus (USB) and other external devices which can be infected by viruses and malware.**

Phishing Attacks

A phishing attack uses email or malicious websites to infect your machine or collect personal and financial data. Phishing emails may appear to come from a real institution or site and may request personal information. When users respond with the requested information or click on a provided link, attackers are then able to access accounts. Several key considerations will help protect you from phishing attempts:

- **Familiarize your staff with the best practices and examples of potential phishing emails described in the CISA PHISHING TIP CARD.**
- **Avoid clicking on hyperlinks in emails. If possible, type the URL into your search bar.**

SECURITY IN PRACTICE

RECOGNIZING PHISHING ATTACKS

Is it Phishing?

1. Does the email appear to come from a real institution but upon further inspection you notice slight adjustments (ex: .net instead of .com, missing letters, etc.)
2. Does the email request that personal information be sent over email or by clicking on a link?
3. Does the email implore you to act quickly to avoid serious consequences?
4. When you hover over a web link, does it go to a site unrelated to the text?

When in doubt, throw it out: *If it looks suspicious, delete it!*

- **Be cautious of emails that offer something that sounds too good to be true or that urge quick action.**
- **Do not reveal personal or financial information in an email and do not respond to email solicitations for this information, including through links sent via email.**
- **Pay attention to the email address or the website URL provided in a suspicious email. Malicious websites and accounts may look identical to legitimate sites and emails but may use spelling variations or different domains.**
- **If it is unclear whether an email request is legitimate, try to contact the company directly or search for the company online—but do not use the information provided in the email!**

Ransomware

Ransomware attacks use malware to deny access to systems or data for the purpose of extortion. After a user has been locked out of the data or system, the malicious cyber actor holds the systems or data hostage until a ransom is paid. Ransomware attacks frequently target end users through phishing emails and unsecured applications. Prevention is the most effective defense against ransomware, so it is critical to consider several precautionary measures:

- **Familiarize your staff with CISA's suite of RANSOMWARE RESOURCES, including the "Combating Ransomware" Webinar and PROTECTING AGAINST RANSOMWARE SECURITY TIPS.**
- **Be wary of opening email attachments, particularly when attachments are compressed files or ZIP files.**
- **For information on protecting your organization's networks and responding to potential ransomware, refer to the RANSOMWARE GUIDE, a customer-centered, one-stop resource with best practices and ways to prevent, protect, and respond to a ransomware attack.**
- **Implement an awareness and training program. Because end users are targets, employees and others who access the network should be aware of the threat of ransomware and how it is delivered.**
- **Ensure all applications and operating systems are regularly updated with the latest security patches.**
- **Install and regularly update antivirus software, firewalls, and email filters to reduce malicious network traffic.**
- **Configure firewalls to block access to known malicious IP addresses which can be found in the NCAS ALERTS AND ANALYTICAL PRODUCTS.**

Website Defacement

A website defacement occurs when an attacker takes control of a public-facing website. HoWs have seen an increasing number of website defacements over the last several years. These types of attacks often feature upsetting imagery and language with the goal of instilling fear in the targeted community and damaging the reputation of the website and its owner. Attacks

on websites can threaten the integrity of the website, as well as the confidentiality of any information tied to the website. To a faith-based organization this can be extremely disruptive and embarrassing. There are several important steps that HoWs can take to protect against website-based cyberattacks:

- **Familiarize your staff with the basics of WEBSITE SECURITY.**
- **Look at services provided by your organization's website hosting provider and contact them to discuss implementing security measures depending on services provided.**
- **Change all default usernames and passwords that were provided from the domain registrar and domain name system (DNS) as these are usually readily available on the Internet and can be used in an attack.**
- **Regularly update the passwords for all accounts on systems that can make changes to your organization's DNS record or website.**
- **Routinely review registrar and DNS records for all domains. Refer to CISA CYBER INSIGHTS: MITIGATE DNS INFRASTRUCTURE TAMPERING for more information.**
- **Enforce multi-factor authentication (MFA) for all authorized users and website administrators.**
- **Enable logging and regularly audit website logs to detect security events or improper access. Unusual or suspicious access should be investigated further.**
- **Regularly scan for and remediate critical and high vulnerabilities. Refer to CISA CYBER INSIGHTS: REMEDIATE VULNERABILITIES FOR INTERNET-ACCESSIBLE SYSTEMS for more information.**

Summary

HoWs are not immune to cyberattacks. An important way to protect your organization is to watch for cybersecurity incidents and report any that you find. CISA offers several widely available services to help organizations of all sizes prepare for and respond to cyber incidents:

- **If your organization experiences an incident, please consider reporting any phishing attempts, malware, or identified vulnerabilities through CISA's SECURE REPORTING TOOL or INCIDENT REPORTING SYSTEM.**
- **CISA analyzes malware, phishing messages, and website or software vulnerabilities to provide actionable information to help citizens better protect themselves in the future.**
- **CISA encourages you to report any activities that you feel meet the criteria for an incident or phishing attack. CISA's policy is to keep all information specific to your organization confidential unless you provide permission to release such information.**

Achieving a culture of cyber readiness requires a new way of thinking about cybersecurity and an investment in prioritizing basic cyber hygiene. Understanding the basics of cyber safety and incorporating simple best practices can make a measurable difference in protecting your facility from damaging cyberattacks. Employees and volunteers should be trained on these best practices and procedures and know how to recognize and act on suspicious activity during a cyber crisis. Cybersecurity should be treated as an extension of other security and contingency plans.

8 Summary and Overall Conclusions

Targeted attacks on houses of worship (HoWs) are a statistically rare but genuine threat to the American people and a major priority for the Department of Homeland Security (DHS). In its capacity as the Nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) has prepared this guide to assist houses of worship and faith-based organizations develop a comprehensive security strategy to help protect life and property.

In this security guide, CISA analyzed ten years of targeted attacks on houses of worship to provide context to the enterprise-wide security recommendations outlined in the previous chapters. The case studies reviewed are examples of the breadth of threats a house of worship faces daily. From physical attacks such as active shooter incidents or bombings to less visible cyberattacks, a house of worship should be vigilant in its security practices.

The best way to mitigate a potential attack is to take a holistic approach to security. This requires assigning clear roles and responsibilities for making security decisions, planning, and implementing the procedures and capabilities across the organization. A robust security plan should be tailored to the specific needs and priorities of the house of worship.

To develop and implement sound security practices, CISA recommends the following options for consideration:

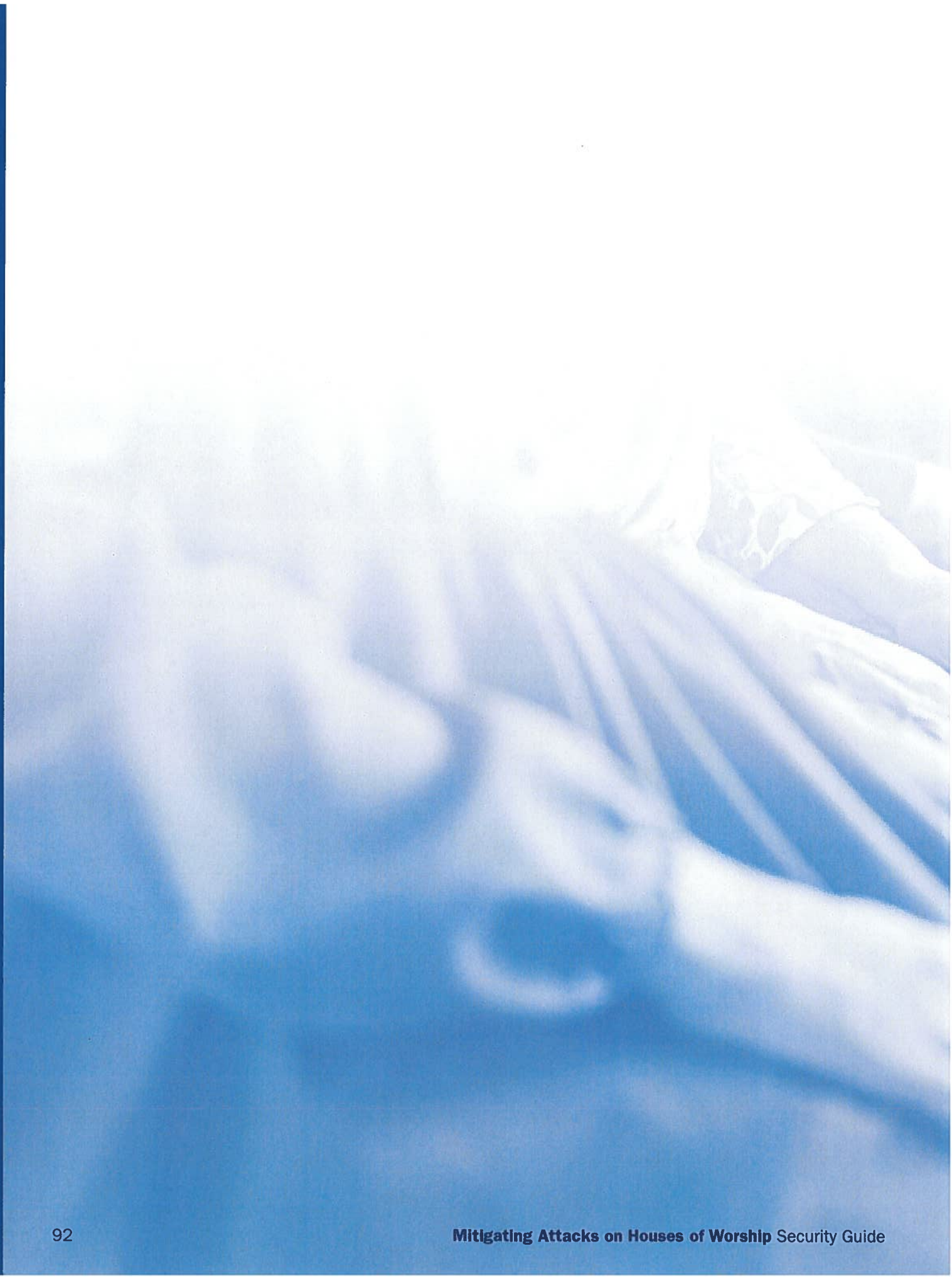
- Establish a multi-layered plan for security, identifying clear roles and responsibilities for developing and implementing security measures.
- Create emergency action plans, business continuity plans, and incident response plans that are well communicated and exercised with the Safety Team for complete understanding.
- Conduct a vulnerability assessment to understand the risks to the house of worship from which you may prioritize implementing any subsequent safety measures.

- Build community readiness and resilience by establishing an organizational culture of caring where all members and visitors are properly supported, and credible threats are reported through previously identified channels.
- Apply physical security measures to monitor and protect the outer, middle, and inner perimeters, while respecting the purpose of each area of the house of worship.
- Focus on the safety of children by implementing safety measures around childcare, daycare, and schools.
- Implement cybersecurity best practices to safeguard important information and prevent a potential cyberattack.

These security options will not deter every threat to a house of worship, but a comprehensive security approach offers the best solution to protect people and property from an attack. HoWs should tailor this knowledge to account for their unique security needs while ensuring the inherent open and welcoming values are maintained.

Looking Forward

CISA will continue to work with faith-based organizations (FBOs) to understand the phenomenon of these types of attacks and provide guidance on ways to mitigate the risk. As CISA looks to the future, it is clear that more study is needed and that some of the most important tangible steps will be to develop a common definition of targeted violence against HoWs, to develop a unified system of tracking and reporting to inform future analysis and security planning, and to continue to link HoWs across the Nation to better share resources, ideas, and solutions.



Appendix 1: Consolidated Resources for Houses of Worship

The resource guide in this section is a consolidation of all the resources provided in this security guide, organized by chapter and section. This list is not exhaustive but provides useful information that can be tailored to any house of worship's (HoW) security plan based on risk and priority.

CATEGORY	RESOURCE
Chapter 1: Introduction	
	DHS, Strategic Framework for Countering Terrorism and Targeted Violence https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence
	FBI, Hate Crime Tracker https://www.fbi.gov/services/cjis/ucr/hate-crime
Chapter 2: Determining a Holistic Approach to Security	
Emergency Preparedness	DHS Hometown Security Report Series for Houses of Worship https://www.cisa.gov/publication/houses-worship-hometown-security-report-series-may-2017
	DHS Guide for Developing High Quality Emergency Action Plans for Houses of Worship https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness
	CISA Active Shooter Emergency Action Plan Template and Guide https://www.cisa.gov/publication/active-shooter-emergency-action-plan-guide
	CISA Active Shooter Emergency Action Plan Video https://www.cisa.gov/active-shooter-emergency-action-plan-video
	CISA Faith Based Organizations - Houses of Worship Security Resources https://www.cisa.gov/faith-based-organizations-houses-worship
	CDC Emergency Action Plan Template https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf
	FEMA Producing Emergency Plan Guidelines https://training.fema.gov/hiedu/docs/cgo/week%203%20-%20producing%20emergency%20plans.pdf
	FEMA Center for Domestic Preparedness https://cdp.dhs.gov/
	FEMA Emergency Kit Checklist https://www.fema.gov/media-library-data/1553273223562-797451b5cb0bee8d35d3e4e85e3830d6/Checklist.pdf
	FEMA Faith-Based Community Preparedness https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness
	American Red Cross First Aid Checklist https://www.redcross.org/get-help/how-to-prepare-for-emergencies/anatomy-of-a-first-aid-kit.html

CATEGORY	RESOURCE
Emergency Operations	CDC Crisis Communication Plan https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf
	CISA Active Shooter Preparedness https://www.cisa.gov/active-shooter-preparedness
	CISA Active Shooter Workshops https://www.cisa.gov/active-shooter-workshop-participant
	CISA Run-Hide-Fight Video https://www.youtube.com/watch?v=W2Vqtf5KqAQ&feature=youtu.be
	CISA Active Shooter Preparedness Video https://www.cisa.gov/options-consideration-active-shooter-preparedness-video
	CISA Active Shooter Training for First Responders https://www.cisa.gov/first-responder
	Ready.gov Active Shooter Resources https://www.ready.gov/active-shooter
	Ready.gov Training Resources https://www.ready.gov/training-0
	Ready.gov "You Are the Help Until Help Arrives" https://community.fema.gov/until-help-arrives
	"Stop The Bleed" https://www.stopthebleed.org/training
	DHS Improvised Explosive Device Training https://cdp.dhs.gov/training/course/AWR-337
	CISA Vehicle Attack Mitigation https://www.cisa.gov/first-responder
	CISA Insider Threat Training https://www.cisa.gov/training-awareness
Business Continuity	Ready.gov Business Continuity Planning Suite https://www.ready.gov/business-continuity-planning-suite
	CISA Active Shooter Recovery Guide https://www.cisa.gov/publication/active-shooter-recovery-guide
	CISA Emergency Services Sector Continuity Planning Suite https://www.cisa.gov/emergency-services-sector-continuity-planning-suite
	CISA Hometown Security: Connect, Plan, Train, Report https://www.cisa.gov/connect-plan-train-report
	FEMA National Continuity Programs https://www.fema.gov/media-library/assets/documents/89510
	DOJ Helping Victims of Mass Violence Toolkit https://www.ovc.gov/pubs/mvt-toolkit/recovery.html

Chapter 3: Conducting a Comprehensive Vulnerability Assessment

	CISA PSAs https://www.cisa.gov/protective-security-advisors
	CISA House of Worship Security Self-Assessment https://www.cisa.gov/publication/houses-worship-security-self-assessment
	EEOC Background Check Guidance https://www.eeoc.gov/background-checks

CATEGORY	RESOURCE

Chapter 4: Building Community Readiness and Resilience

Threat Management	CISA Pathway to Violence Video https://www.cisa.gov/pathway-violence-video
	CISA Pathway to Violence Fact Sheet https://www.cisa.gov/publication/pathway-violence-fact-sheet
	DHS If You See Something, Say Something® Infographic https://www.dhs.gov/see-something-say-something/recognize-the-signs
	DHS If You See Something, Say Something® Pocket Card https://www.dhs.gov/see-something-say-something/campaign-materials
	DHS Risk Factors and Indicators https://www.dhs.gov/publication/risk-factors-and-targeted-violence-and-terrorism-prevention
	CISA Insider Threat: Recognize and Report Anomalous Behavior https://www.cisa.gov/recognize-and-report
	DHS If You See Something, Say Something®: Take the Challenge https://www.dhs.gov/see-something-say-something/take-challenge
	DHS Suspicious Activity Reporting (SAR) Indicators and Examples https://www.dhs.gov/publication/suspicious-activity-reporting-indicators-and-examples
	DHS Nationwide SAR Initiative (NSI) Training: Private Sector Security https://www.dhs.gov/course/nsi-training-private-sector-security
	DHS How to Integrate Suspicious Activity Reporting Into Your Agency's Operations https://www.dhs.gov/publication/10-ways-integrate-sar-your-agency-s-operations
	DHS Nationwide SAR Initiative (NSI): Safety for Faith-Based Events and Houses of Worship https://www.dhs.gov/publication/safety-faith-based-events-and-houses-worship-nsi-awareness-flyer
	FBI Field Office Contact Information https://www.fbi.gov/contact-us/field-offices
	FBI Tip Form https://tips.fbi.gov/
	FEMA Incident Command System (ICS) Resource Center https://training.fema.gov/emiweb/is/icsresource/
Community Engagement and Community Relations	CISA Mass Gatherings: Security Awareness for Soft Targets and Crowded Places https://www.cisa.gov/publication/active-assailant-security-resources
	CISA Patron Screening Best Practice Guide https://www.cisa.gov/publication/patron-screening-guide
	CISA Public Venue Bag Search Procedures Guide https://www.cisa.gov/publication/public-venue-bag-search-guide
	Ready.gov Community Emergency Response Team (CERT) https://www.ready.gov/cert
	DOJ Protecting Places of Worship Forum https://www.justice.gov/crs/our-work/facilitation/protecting-places-of-worship
	Ready.gov "Prepareathon" https://www.ready.gov/prepareathon
	CISA Regional Resiliency Assessment Program (RRAP) https://www.cisa.gov/regional-resiliency-assessment-program

CATEGORY	RESOURCE
Professional Liaison Relationship	Ready.gov Local Emergency Management Information https://www.ready.gov/local
	Tool to Identify Nearest CISA Regions https://www.cisa.gov/cisa-regional-offices
	CISA Protective Security Advisor (PSA) Program Fact Sheet https://www.cisa.gov/publication/psa-fact-sheet
	DHS Federal Protective Service https://www.dhs.gov/topic/federal-protective-service
Mental Health and Social Support Services	MentalHealth.gov "What is Mental Health?" https://www.mentalhealth.gov/basics/what-is-mental-health
	MentalHealth.gov Talk About Mental Health: For Community and Faith Leaders https://www.mentalhealth.gov/talk/faith-community-leaders
	SAMHSA Addressing Risk of Violent Behavior in Youth https://www.samhsa.gov/sites/default/files/addressing-youth-violence.pdf
	SAMHSA FindTreatment.gov https://www.findtreatment.gov/
	SAMHSA Behavioral Health Treatment Services Locator https://findtreatment.samhsa.gov/locator/stateagencies.html#.XurGoG5Fwgo

Chapter 5: Protecting Your Facilities

Grants	FEMA Nonprofit Security Grants Program https://www.fema.gov/grants/preparedness/nonprofit-security
	FEMA Types of Grants https://www.fema.gov/grants
Security Through Design	FEMA Site and Urban Design For Security https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf
	FEMA Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf
Threat Management	FEMA Planning Considerations: Complex Coordinated Attacks https://www.fema.gov/media-library-data/1532550673102-c4846f270150682decbda99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf
	CISA Vehicle Ramming Action Guide https://www.cisa.gov/publication/active-assailant-security-resources
	CISA TRIPwire: Vehicle Born IED Identification Guide: Parked Vehicles https://www.fbiic.gov/public/2008/oct/DHSVehicleBornelEDIdentificationGuideParkedVehicles.pdf
	Office of the Director of National Intelligence (DNI): First Responder Toolbox https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
	CISA Security and Resiliency Guide https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience
	DHS Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings https://www.dhs.gov/science-and-technology/bips-06fema-426-reference-manual-mitigate-potential-terrorist-attacks-against
	FEMA Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings https://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf

CATEGORY	RESOURCE

Chapter 6: Daycare and School Safety Considerations

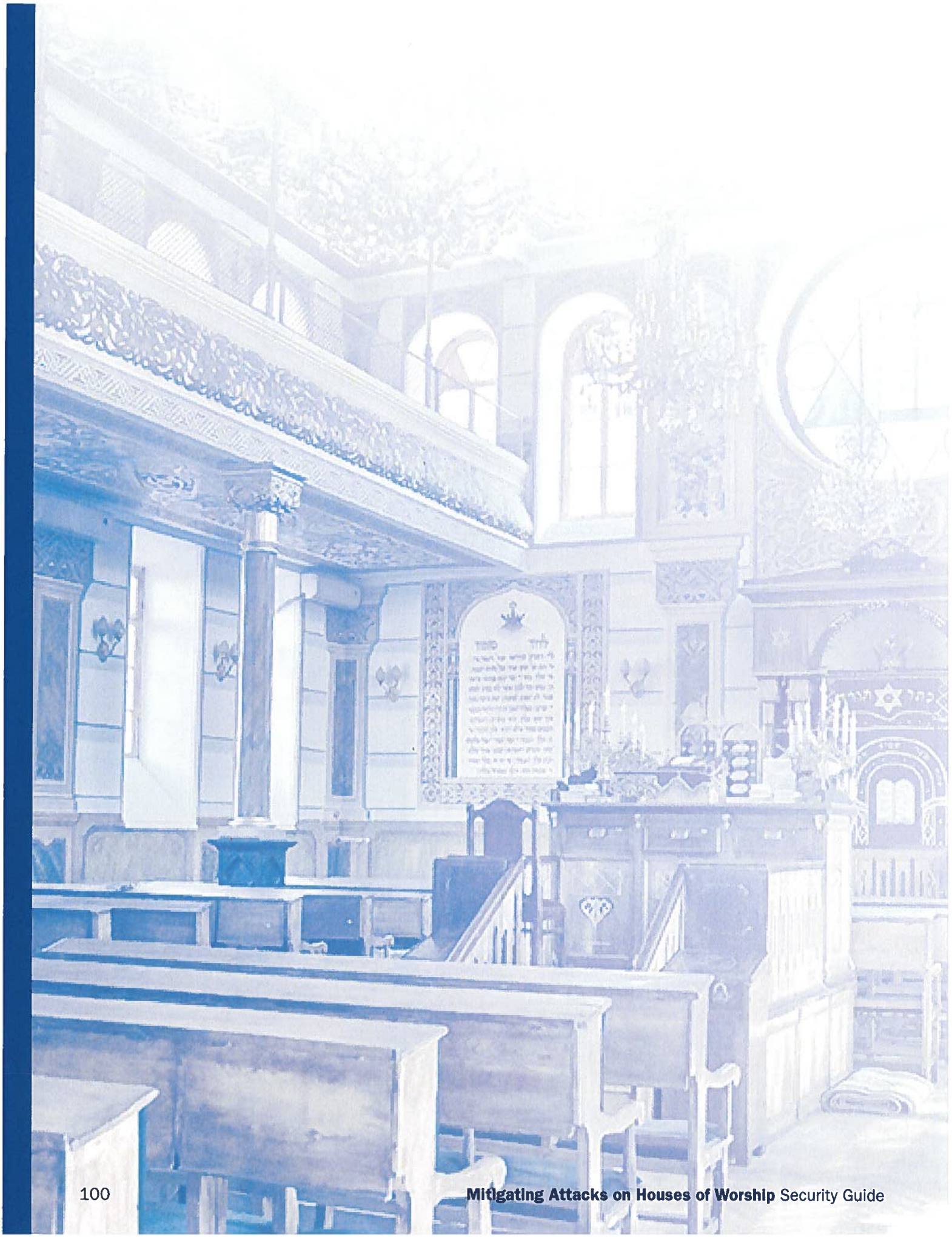
General Resources	DHS SchoolSafety.gov https://www.schoolsafety.gov/
	Department of Education (DoED) Readiness and Emergency Management for Schools (REMS) https://rems.ed.gov/AboutUs.aspx
	SchoolSafety.gov Safety Readiness Tool https://www.schoolsafety.gov/safety-readiness-tool#no-back
	REMS Developing Emergency Operations Plans (EOPS) K-12 101 https://rems.ed.gov/trainings/CourseK12EOP.aspx
	REMS Guide for Developing High-Quality School Emergency Operations Plans https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf
	CISA PSAs https://www.cisa.gov/protective-security-advisors central@cisa.dhs.gov
Physical Security	DHS School Security Survey https://doe.sd.gov/schoolsafety/documents/Security-Survey-508.pdf
	REMS Live Training and Site Assess App https://rems.ed.gov/SITEASSESS.aspx?AspxAutoDetectCookieSupport=1
	Partner Alliance for Safer Schools (PASS): Safety and Security Guidelines for K-12 Schools https://passk12.org/wp-content/uploads/2019/01/PASS-K-12-School-Safety-Security-Guidelines-v4.pdf
School Climate	DoED Guiding Principles: A Resource Guide for Improving School Climate and Discipline https://www2.ed.gov/policy/gen/guid/school-discipline/guiding-principles.pdf
	School Climate Action Guide https://safesupportivelearning.ed.gov/scirp/action-guides
	USSS Analysis of Targeted School Violence https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf
	HHS StopBullying.gov https://www.stopbullying.gov/resources/facts#stats
	USSS Enhancing School Safety Threat Assessment Model https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf
	University of Maryland School Health Assessment and Performance Evaluation (SHAPE) School Mental Health Profile https://www.theshapesystem.com/wp-content/uploads/2019/10/SMH_School-version-10.2.pdf
	HHS Bullying Prevention Assessment Package https://mchb.hrsa.gov/
Training	REMS Live Trainings Request https://rems.ed.gov/TA_TrainingsByRequest.aspx
	DHS Homeland Security Exercise and Evaluation Program https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

CATEGORY	RESOURCE
Funding Resources	DOJ School Violence Prevention Program https://cops.usdoj.gov/svpp
	DOJ STOP School Violence Technology and Threat Assessment Solutions for Safer Schools Program https://bja.ojp.gov/program/stop-school-violence-program/archives
	DoED Project School Emergency Response to Violence (SERV) Violence Recovery Support https://www2.ed.gov/programs/dvppserv/index.html
	DoED E-Rate Program: Cost Effective Technology to Bolster Network Infrastructure https://www2.ed.gov/about/inits/ed/non-public-education/other-federal-programs/fcc.html

Chapter 7: Cybersecurity

Cyber Hygiene	CISA Cybersecurity Resources Roadmap https://us-cert.cisa.gov/resources/smb
	CISA Cyber Essentials https://www.cisa.gov/publication/cisa-cyber-essentials
	CISA National Cyber Awareness System (NCAS): Website Security https://www.us-cert.gov/ncas/tips/ST18-006
	CISA NCAS Using Caution with Email Attachments https://www.us-cert.gov/ncas/tips/ST04-010
	CISA Privacy and Mobile Device Apps https://us-cert.cisa.gov/ncas/tips/st19-003
Online Safety	CISA Online Privacy Tip Sheet https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA NCAS: Staying Safe on Social Networking Sites https://www.us-cert.gov/ncas/tips/ST06-003
	CISA Social Media Cybersecurity Tip Sheet https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA NCAS: Guidelines for Publishing Information Online https://www.us-cert.gov/ncas/tips/ST05-013
	National Cybersecurity Alliance Social Media Cybersecurity Best Practices https://staysafeonline.org/resource/social-media-cybersecurity-best-practices/
	CISA NCAS: Dealing with Cyberbullies https://www.us-cert.gov/ncas/tips/ST06-005
	CISA NCAS: Avoiding Social Engineering and Phishing Attacks https://www.us-cert.gov/ncas/tips/ST04-014
Security Practices and Awareness	CISA How to Recognize and Prevent Cybercrime Tip Card https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA Report Cyber Incidents https://www.cisa.gov/reporting-cyber-incidents https://us-cert.cisa.gov/report
	CISA Sign-up for US-CERT Monthly Bulletin https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new
	CISA Cyber Resilience Review (CRR) https://www.us-cert.gov/resources/assessments
	CISA Cybersecurity Advisors (CSAs) https://www.cisa.gov/csa

CATEGORY	RESOURCE
Security Practices and Awareness (cont)	CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems https://www.cisa.gov/insights
	CISA Cyber Tabletop Exercise Package (CTEP) https://www.cisa.gov/national-cyber-exercise-and-planning-program
	DHS Handbook for Safeguarding Personally Identifiable Information https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information
Malware and Viruses	CISA Malware Tip Card https://www.cisa.gov/publication/stop-think-connect-toolkit
Phishing Attacks	CISA Phishing Tip Card https://www.cisa.gov/publication/stop-think-connect-toolkit
Ransomware	CISA US-CERT Ransomware Resources https://www.us-cert.gov/Ransomware
	CISA NCAS: Protecting Against Ransomware Security Tips https://www.us-cert.gov/ncas/tips/ST19-001
Website Defacement	CISA Cyber Insights: Mitigate DNS Infrastructure Tampering https://www.cisa.gov/insights
	CISA Cyber Insights: Remediate Vulnerabilities for Internet-Accessible Systems https://www.cisa.gov/insights



Appendix 2: List of Incidents

DATE	HoW NAME	DENOMINATION	CITY, STATE
2009			
4/7/2009	Kkottongnae Retreat Camp	Christian	Temecula, CA
John Suchan Chong, 69, a handyman at a Catholic retreat, attacked fellow residents with a handgun in apparent retribution for perceived slights. He shot and killed one victim and injured three others before he was subdued by witnesses.			
2010			
3/20/2010	Church of the Living God	Christian	Pittsburg, CA
John Hugo Scherzberg, 42, set fire to a series of churches because he was angry and blamed God for his life circumstances.			
2011			
6/1/2011	St. Ambrose Cathedral	Christian	Des Moines, IA
Using a covert cyberattack, hackers stole more than $680,000 the diocese raised to help the homeless and abused women.			
2012			
1/1/2012	Imam Al-Khoel Foundation	Muslim	New York City, NY
Ray Lazier Lengend, 40, also known as Suraj Poonai, firebombed a series of residential buildings and houses of worship, including a Hindu temple and a mosque, declaring that he wanted to "take out as many Arabs as possible." No one was injured, but the attacks resulted in significant property damage.			
1/12/2012	Congregation Beth El	Jewish	Paramus, NJ
Anthony Graziano and Aakash Dalal, both age 19 and 20 at the time of their crimes, escalated from a series of anti-Semitic vandalisms to firebombing a pair of synagogues and the home of a rabbi.			
5/12/2012	St. Peter's Episcopal Church	Christian	Ellicott City, MD
Douglas Franklin Jones, 56, shot and killed an Episcopal priest and church secretary in a dispute over the church's food pantry.			

DATE	HoW NAME	DENOMINATION	CITY, STATE
5/20/2012	New Holy Deliverance Outreach Ministry	Christian	Axton, VA

Jean-Claude Bridges, 17, along with an unnamed juvenile co-conspirator, burned down a predominantly black church. At trial, he admitted to targeting the church for reasons of racial prejudice.

8/5/2012	Sikh Temple of Wisconsin in Oak Creek	Sikh	Oak Creek, WI

Wade Michael Page, a 40-year-old Army veteran with ties to white supremacist organizations, shot and killed six people at a Sikh temple. Four other people were seriously injured in the attack, including a responding officer; a priest later died from his injuries. The shooter was wounded by gunfire from responding officers and committed suicide.

8/6/2012	Islamic Society of Joplin	Muslim	Joplin, MO

Jedediah Stout, age 32, was arrested after setting fire to a Planned Parenthood clinic. At trial, he pleaded guilty to several arson charges and confessed to burning down a mosque because he doesn't like Islam.

9/30/2012	Islamic Center of Greater Toledo	Muslim	Perrysburg, OH

Randolph T. Linn, a 52-year-old trucker and former Marine, broke into a mosque after hours and set fire to the prayer room, causing more than $1 million in damages. At trial, Linn confessed that he had been drinking heavily and was upset by sensational news coverage of attacks on U.S. servicemen in the Middle East.

10/1/2012	Temple Kol Ami Emanu-El	Jewish	Plantation, FL

A group of hackers calling themselves Team System Dz took over a synagogue website during a religious holiday and replaced it with anti-Semitic messages and praise for the Islamic State terrorist organization.

10/24/2012	World Changers Church International	Christian	College Park, GA

Floyd Palmer, 51, shot and killed a church volunteer leading a prayer service at an Atlanta-area megachurch. Palmer's motivation is unknown, but he had previously been charged in a shooting at a Baltimore mosque and has a history of mental illness.

12/2/2012	First United Presbyterian Church	Christian	Coudersport, PA

Gregory Eldred, a 52-year-old school teacher, sought out his ex-wife and fatally shot her as she played the organ during a church service. Eldred received a life sentence; his motivation remains under investigation.

DATE	HoW NAME	DENOMINATION	CITY, STATE
2013			
3/31/2013	Hiawatha Church of God in Christ	Christian	Ashatabula, OH
Reshad Riddle, 28, fatally shot his father during an Easter church service and made rambling statements while holding the members at gunpoint. Riddle was quickly subdued by responding officers. A judge found Riddle legally insane and remanded him to the custody of a behavioral health care system.			
10/8/2013	Spring Valley Catholic Church	Christian	Spring Valley, CA
Eugene William Volk, 46, pleaded guilty to a range of charges, including hate crimes and arson, related to a church fire that cause more than $200,000 in damages. Volk had an extensive criminal record and confessed to hating the Catholic faith.			
2014			
4/13/2014	Jewish Community Center of Greater Kansas City	Jewish	Overland Park, KS
Frazier Glen Miller, Jr., a 73-year-old Army veteran with a long history of ties to racist organizations, shot and killed three people at a Jewish community center and retirement community.			
2015			
6/17/2015	Emanuel African Methodist Episcopal Church	Christian	Charleston, SC
Dylan Roof, a 21-year-old white supremacist, shot and killed nine people during a prayer service at a historically black church. During his arrest, Roof stated that his intention was to start a race war.			
9/13/2015	Corinth Missionary Baptist Church	Christian	Bullard, TX
Rasheed Abdul Aziz, 40, entered a church wearing full tactical gear and armed with a handgun, declaring his intention to "slay infidels." The pastor was an experienced crisis intervention specialist and talked the would-be gunman down. He was arrested the following day.			
12/11/2015	Islamic Society of Coachella Valley	Muslim	Coachella, CA
Carl James Dial, 23, threw a Molotov cocktail into a mosque shortly after noon. No one was injured, but the fire caused extensive property damage. Dial's parents described him as troubled, and investigators believe the attack was in retaliation for the 2015 mass shooting attack in San Bernadino.			
2016			
1/1/2016	Islamic Center of Wheaton	Muslim	Chicago, IL
An unknown hacker or group of hackers created a fake website for a Chicago-area mosque, and posted inflammatory images and messages to provoke an anti-Muslim backlash.			

DATE	HoW NAME	DENOMINATION	CITY, STATE
2/28/2016	St. Peter's Missionary Baptist Church	Christian	Dayton, OH

Daniel Schooler, 68, shot and killed his brother, a reverend, during a dispute over a lawsuit. At trial, Schooler explained that he went to the church to discuss the dispute and shot his brother in self-defense after the argument became heated. Schooler had a lengthy criminal record and a history of mental illness.

8/13/2016	Al-Furqan Jame Masjid Mosque	Muslim	New York City, NY

Oscar Morel, 35, shot and killed two Muslim scholars as they exited a New York mosque. A judge sentenced Morel to life in prison, but investigators were unable to determine a motive.

9/1/2016	Hopewell Missionary Baptist Church	Christian	Greenville, MS

Andrew McClinton, 47, burned down a historically black church in Mississippi. McClinton had a lengthy criminal record and investigators concluded that he burned down the church, where he was a member, to cover illicit activities.

9/11/2016	Islamic Center of Fort Pierce	Muslim	Fort Pierce, FL

Joseph Schreiber, 32, set fire to a mosque formerly attended by Omar Mateen, who perpetrated a mass shotting at the Pulse nightclub in Orlando. The mosque was destroyed. Schreiber had previously posted anti-Islamic message on social media and made Islamophobic statements at trial.

2017

1/7/2017	St. Stephen Presbyterian Church	Christian	Fort Worth, TX

Thomas Dale Britton, 54, broke into a church overnight and spent hours several hours vandalizing the building and setting fires, causing more than half a million dollars in damages. He left graffiti attempting to implicate ISIS, but investigators were unable to determine a motive.

2/17/2017	St. Augustin Church	Christian	Des Moines, IA

Ashley Eckhardt, 31, attacked a deacon with a knife during a Catholic ministry for the sick. Witnesses described Eckhardt as disturbed and "yelling about the devil." The deacon survived; a judge sentenced Eckhardt to five years in prison.

6/11/2017	Islamic Society of Tampa	Muslim	Pomona, CA

Shaun Urwiler, a 42-year-old veteran suffering from post-traumatic stress disorder, crashed his truck into several cars and then rammed it through the gate of a mosque, causing about $6,000 in damages. During his arrest, Urwiler told deputies he wanted to "wreak a little havoc."

DATE	HoW NAME	DENOMINATION	CITY, STATE
8/5/2017	Dar al-Farooq (DAF) Islamic Center	Muslim	Bloomington, MN

Three men–Michael McWhorter, 29; Joe Morris, 23; and Michael Hari, 47–attempted to bomb a mosque during morning prayers. McWhorter and Morris pleaded guilty to multiple hate crime charges; Hari is awaiting trial. All three men have ties to white supremacist organizations. The bombing was part of a multi-state crime spree and intended to drive Muslims out of the country.

9/24/2017	Burnette Chapel Church of Christ	Christian	Antioch, TN

Emanuel Kidega Samson, 25, shot and killed one person in the parking lot of the Burnette Chapel Church of Christ in Antioch, TN. Samson proceeded into the church and continued the attach. In total, Samson killed one and wounded seven before law enforcement apprehended him.

11/5/2017	First Baptist Church	Christian	Sutherland Springs, TX

Devin Patrick Kelley, 26, shot and killed 26 and wounded 20 at the First Baptist Church in Sutherland Springs, Texas. He started shooting in the parking lot and moved inside the church to continue the attack. A neighbor to the church with a legal firearm shot Bowers twice, and pursued the assailant in a vehicle. Bowers' vehicle crashed, at which point he committed suicide with a handgun before police could arrive.

2018

10/27/2018	Tree of Life Synagogue	Jewish	Pittsburgh, PA

Robert Gregory Bowers, 46, shot and killed 11 people and wounded six others, including 4 responding law enforcement officers, at the Tree of Life Congregation in Pittsburgh, Pennsylvania. Police exchanged gunfire with the attacker before apprehending him. Bowers faces numerous federal and state charges, including committing a Hate Crime.

11/23/2018	Congregation Bais Yeshuda	Jewish	Los Angeles, CA

Mohamed Mohamed Abdi, 32, used a vehicle in an attempt to run over worshipers exiting Congregation Bais Yeshuda in Los Angeles, California. No casualties were reported. Authorities tracked and arrested the assailant, who shouted anti-Semitic slurs during the attack.

2019

4/1/2019	St. Ambrose Catholic Church	Christian	Brunswick, OH

St. Ambrose Catholic Church in Brunswick, Ohio lost $1.75 million from a renovation fund as the result of a cyberattack. The perpetrators posed as the construction company to hack into the church's email. They used the email access to solicit finance information from another employee.

DATE	HoW NAME	DENOMINATION	CITY, STATE
4/4/2019	**St. Mary Baptist Church/Greater Union Baptist Church/Mount Pleasant Baptist Church**	**Christian**	**Port Barre; Opelousas, LA**

Holden Matthews, 21, burned down four churches in Louisiana over several night. He attacked the St. Mary Baptist Church in Port Barre, LA and Greater Union Baptist Church and Mount Pleasant Baptist Church in Opelousas, LA. Matthews shared videos and images of the attacks on the internet. Matthews faces state hate crime charges.

4/27/2019	**Chabad of Poway Synagogue**	**Jewish**	**Poway, CA**

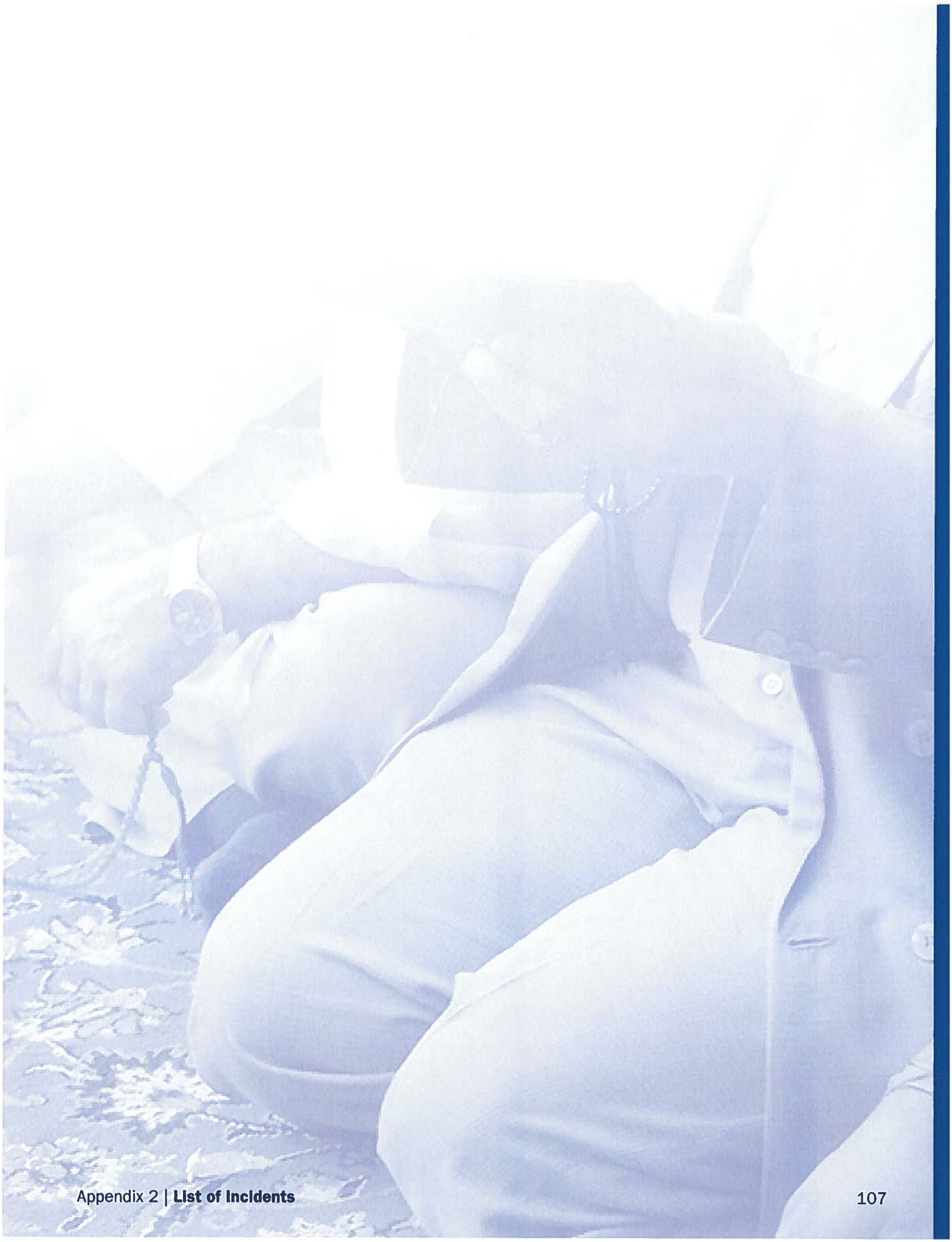
John Timothy Earnest, 19, killed one and injured three in a shooting at the Chabad of Poway Synagogue. The San Diego Police Department apprehended Earnest approximately two miles from the synagogue. The attack occurred on the last day of Passover.

12/29/2019	**West Freeway Church of Christ**	**Christian**	**White Settlement, TX**

Keith Kinnunen, 43, shot and killed two people during a Sunday morning service at a church in White Settlement, Texas. He wore a disguise to carry out the attack. The church's head of security fatally shot Kinnunen.

12/29/2019	**Congregation Netzach Yisroel**	**Jewish**	**Monsey, NY**

Grafton Thomas, 37, is accused of attacking several people with an edged weapon at a Hanukkah celebration hosted by a Rabbi in Monsey, New York. He was declared unfit to stand trial and is currently at a mental care facility.



U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

Washington, D.C. 20528

DEPARTMENT OF PLANNING
KA'ĀINA HULL, DIRECTOR
JODI A. HIGUCHI SAYEGUSA, DEPUTY DIRECTOR

DEREK S.K. KAWAKAMI, MAYOR
REIKO MATSUYAMA, MANAGING DIRECTOR

Kaua'i County Historic Preservation Review Commission (KHPRC)

DIRECTOR'S REPORT

I. SUMMARY

Action Required by KHPRC:

- Consideration of a Class I Zoning permit for proposed exterior additions to an existing historic church.

KHPRC action may include the following:

1) Support for the project as represented; or
2) A recommendation that its approval of the project should incorporate conditions of approval; or
3) A recommendation to consider denial of the permit; or
4) A recommendation to defer action on the permit

II. PROJECT INFORMATION

Permit Numbers	HPRC-2023-20 Class I Zoning Permit Z-XX-2024 Building Permit BP-2024-XXX		
Parcel Location:	Kōloa, Kaua'i		
Tax Map Key(s):	(4) 2-8-010:008	**Area:**	2.6000 acres/ 113,256 sq. ft.
LAND USE DESIGNATIONS & VALUES			
Zoning:	T4-VC		
State Land Use District:	Urban		
General Plan Designation:	Neighborhood Center		
Owner(s)/ Applicant:	The Church at Kōloa		

III. PROJECT DESCRIPTION

H.1.a.

AUG 17 2023

The Applicant, the Church at Kōloa, is the owner of the subject property located in Kōloa Town. The Applicant is proposing several exterior additions to the historic church that include the following:

- **Side Exterior Additions**
  The Applicant is proposing to expand its footprint with two exterior additions that will be located to each side of the church building. Each bump out addition will involve a 2-story expansion with approximately 130 square feet in size.

  The left addition, which will be accessed through the existing lounge room, will accommodate an ADA restroom on the first floor and an attic space on the second floor. The right addition, which will connect from the men's restroom and AV room, will provide an interior staircase and exterior exit to provide the security team with a more convenient access to the security surveillance room on the second floor.

  As represented, the Applicant is proposing the new additions as a precautionary measure to mitigate against future attacks to the church after experiencing some issues with trespassing and homelessness onto the church property. The ADA restroom improvement is needed to accommodate members who are elderly, wheelchair bound, or physically impaired.

- **Emergency Exit Doors**
  The Applicant is also proposing two emergency exit doors with stairs and a concrete landing pad to provide additional exits for members in case of an emergency event. The proposed emergency exits will be located on both sides of the church and will involve the removal of a portion of the exterior window and the installation of new french doors.

The church owns adjacent properties on TMK: 2-8-010:009 and TMK: 2-8-010:010 that have several single-family residences and other accessory structures. For purposes of this application, the KHPRC review will focus on the church structure and its surrounding area that is located on TMK: 2-8-010:008.

IV. TRIGGER FOR KHPRC REVIEW

Hawai'i Revised Statutes (HRS) §6E-2 defines "Historic property" as "any building, structure, object, district, area, or site, including heiau and underwater site, which is over fifty years old."

Hawai'i Administrative Rules Title 13 defines "Significant Historic Property" as "any historic property that meets the criteria" for listing on the Hawai'i Register of Historic Places under HAR 275-6(b) or HAR 2846(b).

- **Site/Building/Structure/Object IS NOT Listed on the National or State Historic Register.**
- **The subject property is NOT located in a Historic District, but may qualify as a contributing building towards a Historic District designation.**
- **The church building IS over 50 years old and IS by law defined as a "historic property."**
- **The subject property IS included on the KHPRC Inventory List.**

V. PROJECT HISTORY AND BACKGROUND

- **Church History**
  According to the church website[1], the existing church was constructed in 1859 to replace the original church building (1837-1859) that was destroyed. In 1929, the existing church structure underwent repairs including a New England style finish with changes to the front façade.

- **Zoning Permit History**
  The Department maintains the following zoning permits that are associated with the subject property. Of the permits listed, only some of the permits are directly associated with the church structure and noted in the table below in the underlined text.

Table 1. Zoning Permit History

Year	Zoning Permit Number	Permit Description
1969	R-276	Bath, Cafeteria, dormitory
1969	R-363	New Parsonage
1974	***Z-4444-1974***	***Office Addition to the Church Structure***

[1] History | The Church At Kōloa (thekoloachurch.com)

	B-684-3-74	
1976	Z-248-1977 B-337-10-77	Enclose Lanai
1978	Z-598-1979	SFR relocated from a Different Parcel
1979	Z-1000-1079	Relocate 2 residence
1984	Z-519-1985	Relocate existing residence in the same parcel
1987	Z-III-1987-6	8th Dwelling
1987	Z-1068-1987	Garage Addition to a Residence
1993	***R103134***	***Repair of Roof and New Trusses on the Church***
1993	***R103134 Addendum #1***	***Replace Steeple on the Church***
1993	***R103134 Addendum #2***	***New Meeting Room Addition to the Church***
1993	R104321	Carport/ Storage
1995	Z-III-1995-9	Education Building with 2 residential units
2005	***Z-750-2005***	***New Roof Addition over the Existing Deck***

Of the zoning permits the Department maintains, only a handful are specifically related to the church structure. In 1974, the Applicant constructed an office addition that is attached to the left rear corner of the existing church building. In 1993, the Applicant applied for OEP permits in response to damages and repairs associated with Hurricane Iniki. The OEP permits were for improvements to the church building including the repair of the roof, addition of new trusses, replacement of the steeple, and the addition of a new meeting room. In 2005, the Applicant constructed a roof addition over the existing deck to the left rear side of the church building.

VI. EVALUATION OF HISTORIC SIGNIFICANCE

- **Criteria for Nominations to the Hawai'i Register of Historic Places:**

Pursuant to HAR Section 13-198-8, in deciding whether a property should be entered and ordered into the Hawai'i register, the review board shall evaluate whether the property meets or possesses, individually or in combination, the following criteria or characteristics:

(1) The quality of significance in Hawaiian history, architecture, archeology, and culture, which is present in districts, sites, buildings, structures, and objects of State and local importance that possess integrity of location, design, setting, materials, workmanship, feeling, and association, and:

(A) That are associated with events that have made a significant contribution to broad patterns of our American or Hawaiian history;

The subject property is **likely** to be associated with events that have made a significant contribution to broad patterns of Hawaiian history. As represented on the church's website, the subject property served as the first mission station in Kōloa Town. The original chapel, constructed in 1837 and situated on land granted by King Kamehameha III, was attended by Native Hawaiians near and far who traveled by foot or horseback to hear the word of God. It is estimated that the early church had between nine to fifteen hundred people.[2]

(B) That are associated with the lives of persons significant in our past;

The subject property **may be** associated with the lives of persons significant in our past. The Reverend Peter J. Gulick, who lived in Waimea, was one of the first missionaries to arrive on Kaua'i and who led the charge for establishing a mission station in Kōloa Town in 1835.[3] The church was also associated with Reverand James W. Smith who was a missionary, pastor, and doctor and was instrumental in overseeing the completion of the church building in 1859.[4]

(C) That embody the distinctive characteristics of a type, period, or method of construction, or that represent the work of a master, or that possess high artistic value, or that represent a significant and distinguishable entity whose components may lack individual distinction; or

---

[2] History | The Church At Kōloa (thekoloachurch.com)
[3] Hoverson, Martha. *Historic Kōloa : a Guide*. The Friends, 1985.
[4] History | The Church At Kōloa (thekoloachurch.com)

The subject property **is** eligible for listing based on Criteria C. Based on the Department's research, the church building continues to uphold a New England style architecture that is representative of the early churches that were built in Hawai'i.[5] Although the front façade of the church was modified in 1930 with the addition of the portico and spire, the additions have become contributing character defining features to the church building.[6]

(D) That have yielded, or may be likely to yield, information important in prehistory or history;

The subject property **may be** likely to yield information important in prehistory or history, especially as it pertains to the influence and impact of the first missionaries on Kaua'i between 1820 through the mid-1930s.

- **Evaluation of Historic Integrity:**

The existing church building **retains** historic integrity through its location, setting, design, materials, workmanship, feeling, and association.

Although renovations were done in 1930 to update the front façade, the modifications have become contributing character defining features that have added to the iconic look of the church. The permit history, as outlined above, also verifies additions that have been constructed over the years. However, many of the later additions were located at the rear of the historic church and in doing so did not detract from the historic integrity of the front façade.

- **Evaluation of Secretary of Interior Standards for Rehabilitation**

The National Park Service offers Preservation Brief #14 to provide guidance on new exterior additions to historic buildings. In summary, the proposal should take into consideration the following:

- Can the proposed addition be accommodated within the existing footprint in a manner that does not affect any character defining features of the interior space?

Department's Evaluation:

[5] Hoverson, Martha. *Historic Kōloa : a Guide*. The Friends, 1985.
[6] Hoverson, Martha. *Historic Kōloa : a Guide*. The Friends, 1985.

Based on a further review of the site plans and a site visit conducted in July (see site visit photos attached as Exhibit A), the Department has strongly encouraged the Applicant to explore alternatives to the bump out additions. Alternatives to consider include trying to accommodate the proposed additions within the existing footprint by:

1) relocating the security room to the existing office addition; and
2) converting the existing women's restroom and lounge room into the ADA restroom.

- If an exterior addition is necessary, then the proposed addition should align with Standards 9 and 10 of the Standards for Rehabilitations which state:

(9) New additions, exterior alterations, or related new construction shall not destroy historic materials that characterize the property. The new work shall be differentiated from the old and shall be compatible with the massing, size, scale, and architectural features to protect the historic integrity of the property and its environment.

(10) New additions and adjacent or related new construction shall be undertaken in such a manner that if removed in the future, the essential form and integrity of the historic property and its environment would be unimpaired.

Department's Evaluation:
Based on the Department's review, the Applicant is proposing the additional bump outs after exploring alternative design options. The Applicant asserts that the proposed additions are needed to better accommodate the growing needs of the church that cannot be contained within the existing footprint. If additions are warranted, the Department maintains the position that additions should be in keeping with the Secretary of Interior standards by trying to locate new additions towards the rear of the property and set away from the front façade of the building.

VII. ADDITIONAL FINDINGS

- The Department finds that the proposed application, as represented, would drastically alter the historic integrity of the church which is known for its iconic street front façade.

- The Department is currently in conversation with the Fire Department and the Building Department to verify the building and fire code requirements for the proposed emergency exits. The Department has been in conversations with the Applicant and would like the Applicant to explore alternative locations that would not alter the original windows.

VIII. RECOMMENDATION

Based on the foregoing evaluation, the Planning Department recommends that the Kaua'i Historic Preservation Review Commission **DEFER** the proposed application as represented and requests the Applicant to return to the commission with a revised plan that takes into consideration the following:

- Explores and exhausts alternative designs that comply with the Secretary of Interior Standards of Rehabilitation. Specifically, the Applicant should consider trying to accommodate the proposed improvements within the existing footprint. Furthermore, if the additions cannot be accommodated within the existing footprint, then the Applicant should submit an alternative design that locates the additions to the rear of the building.

- The Applicant should also explore alternative locations for the two emergency exit doors that will not affect the original windows or any other character defining feature.

The Commission is further advised that this report does not represent the Planning Department's final recommendation in view of the forthcoming public hearing process whereby the entire record should be considered prior to decision making. The entire record includes but is not limited to:

a. Government agency comments;

b. Testimony from the general public and interested others; and

c. The land owner's response.

By _____
MARISA VALENCIANO
Planner

Approved & Recommended to Commission:

By _____
JODI A. HIGUCHI SAYAGUSA
Deputy Director of Planning

Date: 8-8-2023

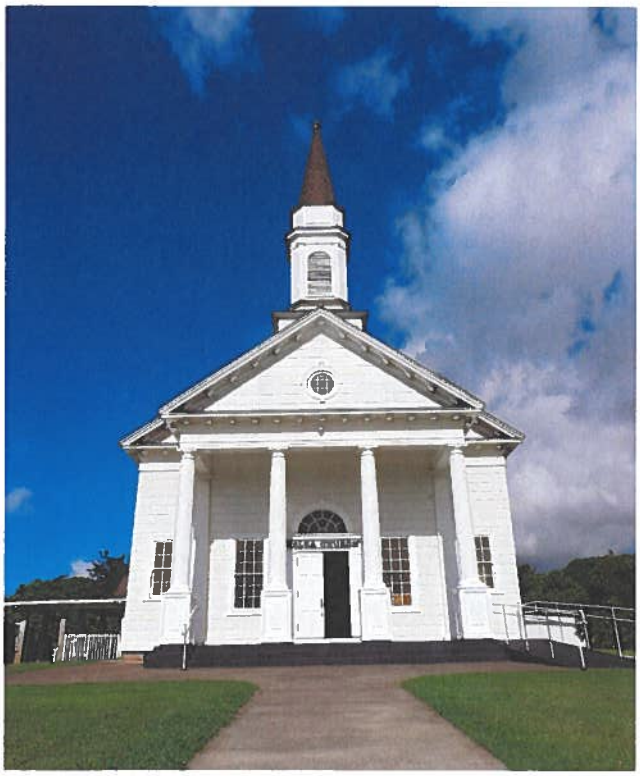
Exhibit A

The Church At Koloa

Planning Department Site Visit for KHPRC Director's Report
Site Visit Date: July 28, 2022 @ 9:00am

TMK: 2-8-010:008
Proposed Additions to the Existing Historic Church

Exterior- Street Front View



Exterior- East View

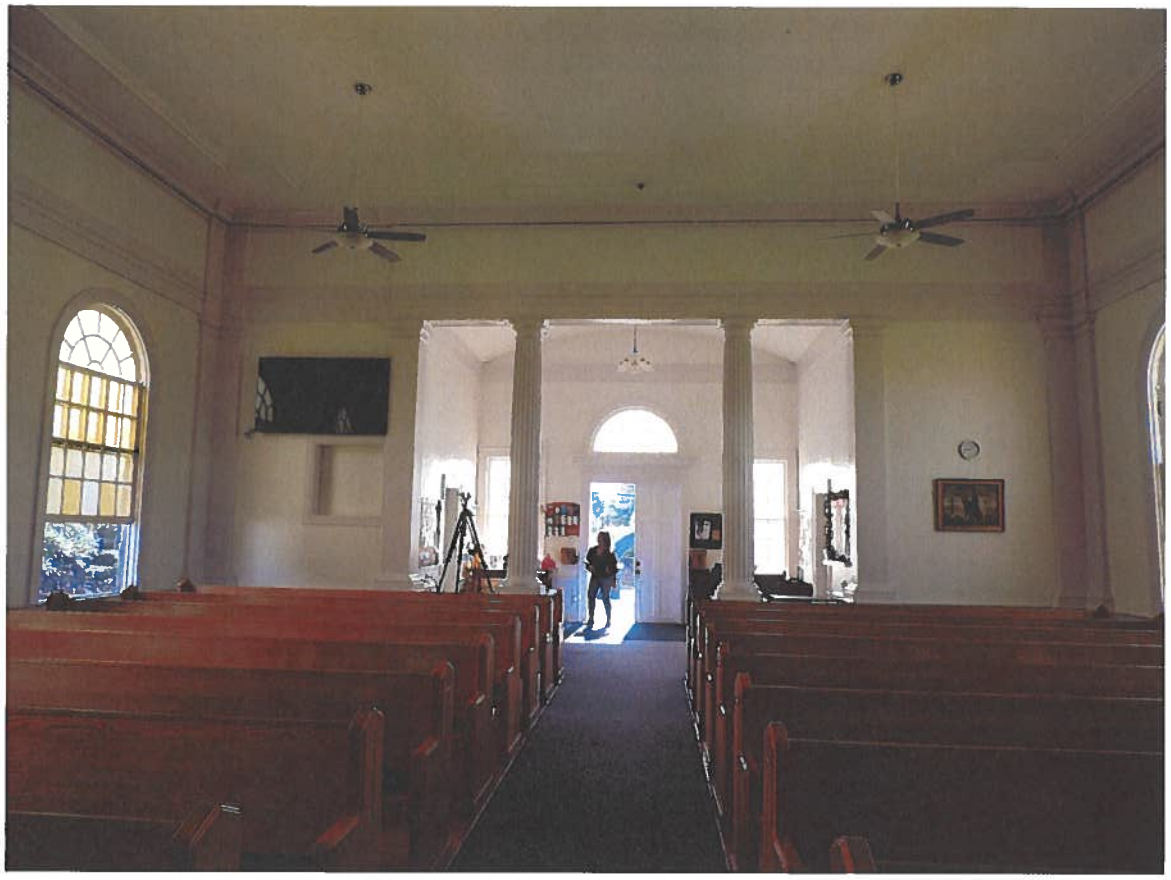
Exterior- Rear View

Exterior- West View

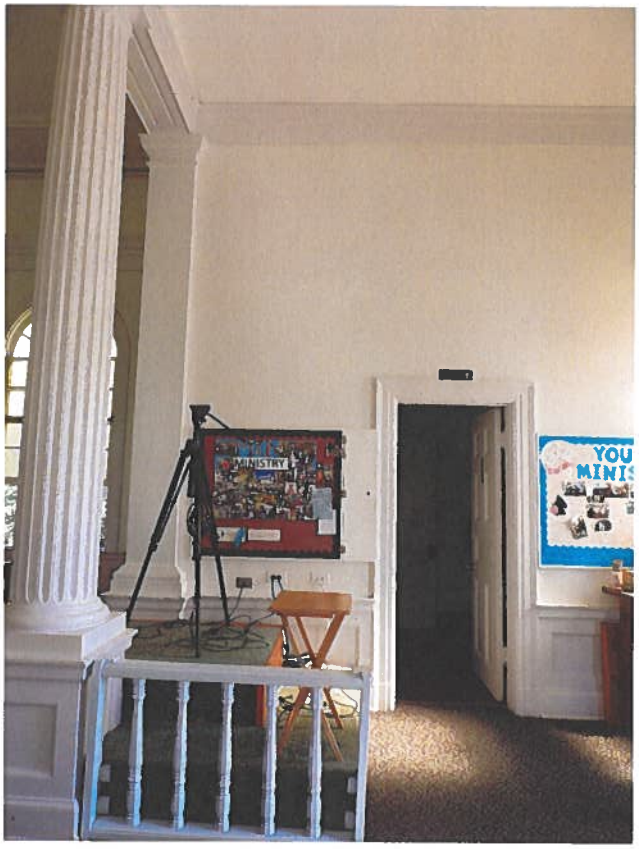
Exterior- West View

Interior- View from Front Door and facing the stage

Interior- View from the stage facing towards the front door

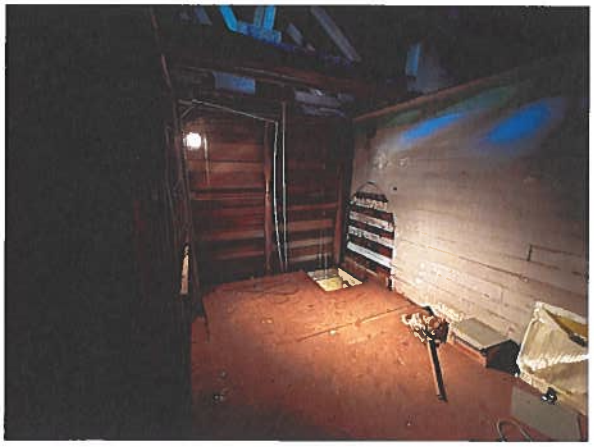


Interior- Women's and Men's Restroom to the sides of the front door



Interior-AV Room located across from the Men's Restroom

Interior- Above AV Room and Men's Restroom



Existing space above the AV room and the Men's restroom and accessed through the stairs in the AV room.