FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Monthly Newsletter

June 2026
Volume 8, Issue 6

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: SEVERE

FB-ISAO Physical Threat Level for US Faith-Based Organizations: "**SEVERE**."

FB-ISAO's definition of the Physical Threat Level, " **SEVERE** " means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is highly likely.

FB-ISAO Cyber Threat Level: ELEVATED

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as "ELEVATED."

FB-ISAO's definition of the Cyber Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is more likely than normal.

Board of Advisors

Contact Us

Email

Website

How to join

Join FB-ISAO Slack Channel

FB-ISAO Events page

Independence Day 250th Anniversary

The July 4, 2026, Independence Day holiday marks the 250th anniversary of the signing of the Declaration of Independence, creating a larger and more symbolic celebration environment across the United States. America250 identifies July 3–5 as a major commemoration period, with signature events in New York City, Philadelphia, and California, plus Main Street celebrations nationwide. For Houses of Worship (HOWs), Faith-Based Organizations (FBOs), nonprofits, and other community-serving organizations, the concern is not limited to official venues or hosted events. Nearby parades, fireworks, demonstrations, road closures, crowd movement, drones, severe weather, and emergency response activity may affect facilities, staff, volunteers, visitors, congregants, tenants, customers, and continuity of operations.

HOWs and FBOs may host patriotic services, outreach events, volunteer activities, community meals, concerts, or prayer gatherings, while others may simply be located near activity that changes the operating environment. Smaller staffs, volunteer-based operations, and holiday schedules can make advance coordination especially important.

Large public celebrations can extend beyond formal event boundaries. People may use nearby parking lots, sidewalks, lobbies, restrooms, transit stops, shared entrances, and public plazas before, during, and after events. Facilities may also experience blocked entrances, increased restroom or shelter requests, delivery delays, staff access challenges, unattended items, medical calls, protest activity, confusion caused by fireworks, or reports of suspicious drone activity. These impacts can occur even when the activity is lawful, celebratory, and not directed at the organization.

MITIGATION. Before the holiday period, HOWs, FBOs, nonprofits, and other community-serving facilities should review public gathering, exterior security, and continuity plans. CISA has published resources for venues preparing for major 2026 events, including guidance tied to bombing prevention, venue security, public gathering security, and dependency disruption planning that may also be useful. A few recommended actions include:

- Review local event activity
- Map the surrounding footprint
- Coordinate with local authorities
- Adjust staffing and access control
- Prepare for crowd spillover
- Monitor exterior spaces
- Review vehicle and pedestrian separation
- Plan for fireworks and drones
- Update communication plans

Voice Phishing (Vishing)

Vishing, or voice phishing, remains a persistent social engineering threat because it targets people, trusted relationships, and everyday business processes. Attackers may use phone calls, text messages, voicemails, fake IT support scenarios, credential harvesting pages, and unauthorized cloud applications to pressure staff or volunteers into sharing credentials, approving multifactor authentication (MFA) prompts, changing payment details, resetting accounts, or authorizing access to software and/or cloud platforms. For Houses of Worship (HOWs), faith-based schools, nonprofits, and other community-serving organizations, the risk is practical: public-facing contact information, donor and member relationships, outsourced services, and a culture of helpfulness can make malicious calls sound credible and urgent.

Vishing succeeds when urgency, trust, and informal processes override verification. HOWs and other faith-based organizations can reduce risk by slowing down sensitive requests, confirming identity through trusted channels, limiting exceptions, monitoring cloud access, and reinforcing that verification is a normal part of protecting the community. Therefore, it's important to be cautious of unexpected calls or messages that create urgency, ask staff/volunteers to bypass normal process, request passwords or MFA codes, direct users to unfamiliar login pages, ask for approval of connected applications, request payment or payroll changes, claim a leader or vendor needs immediate action, or pressure help desk personnel to reset credentials or enroll a new device. Voice alone should not be treated as proof of identity, especially for financial, account recovery, or other sensitive requests.

MITIGATION. The goal is not to eliminate phone communication, but to reduce the chance that a single convincing call can override security controls. Organizations can reduce exposure by making verification normal, repeatable, and encouraged by leadership by:

- Verifying sensitive requests through a trusted channel
- Securing account recovery
- Controlling data access
- Protecting financial workflows
- Training beyond email phishing
- Limiting help desk exceptions
- Using phishing-resistant MFA where feasible

Spotlight:

Take9 is a nonprofit organization dedicated to helping people stay safer online by promoting one simple but powerful habit: *count to 9 before you click*. By encouraging people to take nine seconds to stop and think before clicking a link, responding to a message, or sharing personal information, Take9 helps individuals avoid scams that rely on urgency, fear, and impulsive reactions.

From vishing, phishing emails, and fake text messages to impersonation scams and suspicious links, Take9 equips people with the tools and confidence to spot red flags before it's too late. At the core of every campaign is the belief that a short pause can make a meaningful difference in protecting yourself, your family, and your community online.

Take9 is funded by craig newmark philanthropies and supported by Aspen Digital.

FB-ISAO is a partner of Take9

Thank you for sharing this newsletter with a friend!