FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Monthly Newsletter

January 2026
Volume 8, Issue 1

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: ELEVATED

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

FB-ISAO's definition of the Physical 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.

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

AI Deepfake Impersonation Scams Targeting FBOs

Faith communities are increasingly being targeted by AI-generated deepfake impersonation scams, in which attackers clone the voices or likenesses of pastors to deceive congregants into sending money or taking other actions. Recent incidents demonstrate that scammers have successfully used synthetic audio that convincingly imitates pastors' voices to solicit fraudulent donations from members of their congregations.

Actively Targeting FBOs. Attackers are leveraging AI voice-cloning technology to transform publicly available sermon recordings, livestreams, and online media into convincing synthetic messages that replicate pastors' voices, tone, and cadence.

Low Technical Barrier, High Trust Exploitation. These impersonation scams require little technical sophistication. Rather than compromising systems or accounts, attackers exploit the availability of public audio content and widely accessible AI tools, combined with the high level of trust congregants place in communications from clergy.

Financial & Reputational Risk. The most immediate impact of these scams is direct financial loss through diverted donations or fraudulent payments. Beyond financial harm, successful impersonation scams can undermine congregational trust in leadership communications.

Human-Layer Vulnerability. Even congregants familiar with a pastor's voice may struggle to distinguish authentic communications from AI-generated impersonations, particularly when messages are brief, urgent, or emotionally framed.

CONSIDERATIONS. AI-generated impersonation scams exploit trust, not technology gaps. Faith communities can reduce exposure to AI-enabled impersonation scams by prioritizing verification, awareness, and communication discipline, particularly around financial requests and urgent messaging.

- Assume voice and video can be fabricated
- Establish clear verification protocols for financial requests
- Limit reliance on urgent or informal payment appeals
- Educate congregants on red flags
- Protect leadership digital footprints where feasible
- Prepare a rapid response plan for suspected impersonation

Additional Security Considerations for Religious Events Held in Public Spaces

These considerations are offered in light of the Bondi Beach attack in Sydney, Australia on the first night of Hanukkah. Broader relevance for FB-ISAO stakeholders lies less in the specific attack vector and more in the operational context highlighting the heightened security risks of hosting large gatherings in open, recreational spaces not designed for protective measures.

From an analytical standpoint, the event's openness and location are central to understanding both the vulnerabilities exploited and the challenges encountered.

Unlike controlled environments such as private facilities, public venues often lack defined perimeters, controlled access, and hardened shelters, complicating detection, response, and evacuation, shaping both threat opportunity and defensive feasibility.

Unfamiliar Venues Increase Risk. Public spaces like beaches lack defined perimeters, controlled access, and hardened shelters, making them harder to secure compared to religious facilities or other private venues.

Situational Awareness Challenges. Open areas introduce multiple access points, elevated vantage positions, and adjacent zones that are difficult to monitor. Crowd behavior in recreational settings—marked by distraction and fluidity—reduces threat detection and response speed.

Human Factors. Attendees unfamiliar with security measures may fail to recognize warnings or suspicious activity, complicating evacuation and emergency response.

Limitations of Traditional Security. Measures such as screening or barriers may be impractical or culturally disruptive in open settings. Coordination with local law enforcement and municipal authorities is critical for tailored patrols and rapid response planning.

Resource Gaps. Physical and logistical resources (shelter, lighting, medical access) differ significantly from controlled environments, requiring reassessment during planning.

Implications. Adversaries may exploit symbolic, open spaces where security controls are diluted. While public events should not be curtailed, they require context-specific planning and realistic protective strategies.

Spotlight: FB-ISAO Slack! Do you Still Need to Check it Out?

Volunteers tasked with leading security programs at their houses of worship have found great benefit from networking with others in similar roles. FB-ISAO Slack offers such an opportunity. On FB-ISAO Slack, members share things like Suspicious Activity Reports (SARs), resources, and ask questions. **Have you joined yet?**

Join today and experience the benefits of membership and increased resilience for your house of worship in 2026:

- ➤ Collaborate on FB-ISAO Slack.
- ➤ Analytical and incident reports on security topics.
- ➤ Join live discussions and access our recording library
- ➤ Access community-centric and community-developed best practices.

Thank you for sharing this newsletter with a friend!