FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Monthly Newsletter

March 2026
Volume 8, Issue 3

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

Preoperational Surveillance Awareness

For houses of worship and other faith-based organizations, situational awareness can be a community-centric responsibility. Faith-based organizations often emphasize openness and hospitality, which can unintentionally obscure early reconnaissance behaviors. Incorporating structured surveillance indicators helps positions like greeters, ushers, and volunteer hosts recognize patterns that are inconsistent with mission activities and report them, while maintaining community trust and respect.

In February, the Joint Counterterrorism Assessment Team (JCAT) released Awareness of Preoperational Surveillance Tactics Associated With Terrorism Offers Opportunities, a resource outlining reconnaissance behaviors that often precede attack planning. Additional guidance to help understand these indicators can also be found in the CISA "Power of Hello" and Gate 15's Hostile Event Attack Cycle.

Surveillance and reconnaissance activities occur in the preoperational planning phase, sometimes well before violence ensues. The JCAT resource highlights a range of behaviors that may be benign in isolation but become meaningful when repeated or combined, including:

- Repeated presence near sensitive access areas
- Persistent photography or videography of building infrastructure
- Detailed notetaking or mapping around security features
- Testing or probing doors, locks, or access points

Understanding these indicators as part of a larger pattern, rather than isolated actions, enhances the ability to discern risk.

Strengthening situational awareness requires practical guidance, consistent training, and accessible reporting mechanisms that frontline staff and volunteers can apply confidently and accurately.

- Train frontline personnel using structured indicators.
- Establish behavioral baselines for normal operations.
- Teach pattern recognition rather than single indicators.
- Implement clear reporting and escalation protocols.
- Encourage respectful engagement strategies.
- Coordinate with external partners.

Insider Threat Prevention

For faith-based organizations, insider-threat prevention carries distinct operational importance. These environments often rely on trusted staff, volunteers, and third-party partners, while maintaining open and collaborative cultures that may reduce friction around access and information sharing. As a result, negligent handling of data, credential compromise, or misuse of authorized access can have disproportionate reputational, legal, and community-trust impacts. Strengthening insider-risk governance, without undermining mission-driven openness, requires balanced controls, awareness, and leadership engagement tailored to community-centric operating models.

Why Insider Threats Persist. Insider threats, originating from individuals with authorized access to systems, facilities, or sensitive data, remain a persistent and costly risk for organizations across all sectors. These threats may be malicious, negligent, or compromised. Whether through negligence, coercion, or intent, insiders can exploit legitimate privileges in ways that external attackers cannot easily replicate.

CISA's POEM (Plan-Organize-Execute-Maintain) framework, published in January 2026, offers a practical structure for assembling and sustaining insider-threat management teams across disciplines.

MITIGATION. Because insider threats arise from trusted access rather than external intrusion, prevention requires governance, culture, and technology working together. The following actions prioritize practical, scalable measures applicable across organizational sizes and sectors.

- **Establish Cross-Functional Governance.** Create a formal insider-threat working group spanning leadership, HR, legal, cybersecurity, and security operations, aligned to POEM-style lifecycle management.
- **Strengthen Identity, Access, and Monitoring Controls.** Apply least-privilege access, continuous logging, and behavioral monitoring aligned to authoritative frameworks.
- **Expand Workforce Awareness and Reporting Culture.** Promote training that addresses negligence, phishing susceptibility, and safe data handling while encouraging early reporting of concerns.
- **Integrate Insider Scenarios into Incident Response.** Ensure response plans include playbooks, legal considerations, and evidence preservation specific to insider-driven incidents.

Spotlight: FB-ISAO Education Sessions Continue

If you haven't participated in any FB-ISAO education sessions for members, please consider joining the 2026 series on **Building and Intelligence Function for Houses of Worship**. Our sessions are recorded and made available to members. However, there's no substitute for being part of the conversation where you can share your own experiences, ask questions, and most importantly engage with the community of your peers grappling with similar challenges!!

- ➤ This most recent event series kicked off in January and continues through June. Please consider joining as we delve into how a deeper understanding of the intelligence process better informs resilience-building activities.
- ➤ Previous series discussed FireArms in the House and Standing Up Teams.
- ➤ Our recording library is available to members on the FB-ISAO Slack workspace.

Thank you for sharing this newsletter with a friend!