FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Monthly Newsletter

April 2026
Volume 8, Issue 4

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

Executive/VIP Protection

A recent Joint Counterterrorism Assessment Team (JCAT) product titled Enhancing Security for High-Profile Figures as Public Gatherings highlights how public appearances, particularly those that are open, community-oriented, or widely advertised, create conditions where protective measures must operate across multiple domains and stakeholders.

Houses of Worship (HOWs) naturally align with many of the conditions that increase risk for executive protection. Worship services, conferences, and community events are often open, widely accessible, and publicly promoted, creating predictable environments with large and dynamic attendance. At the same time, organization leaders and guest speakers are highly visible and frequently public facing, with their presence and schedules often shared in advance. Together, this combination of accessibility, predictability, and identifiable VIP presence reflects many of the risk factors outlined in the JCAT assessment, increasing exposure and reinforcing the need for deliberate security planning.

Expanded Exposure. Public gatherings often involve large crowds, multiple entry points, and limited ability to fully screen attendees. The combination of visibility and accessibility creates conditions where even low-capability actors can exploit opportunity, increasing the importance of proactive risk identification.

Coordination Gaps. Coordination challenges across multiple stakeholders, including law enforcement, private security, venue staff, and event organizers represent a primary systemic vulnerability. Even well-resourced security plans can fail if integration across stakeholders is insufficient.

Access Vulnerabilities. Temporary staff, contractors, and volunteers introduce additional risk into event environments. These individuals often have legitimate access but may not be subject to the same level of vetting or oversight as permanent personnel.

Digital Exposure. Publicly available information about events, including timing, location, and VIP attendance, can be leveraged by threat actors for pre-operational planning. Digital exposure acts as an early-stage enabler of physical threat activity.

MITIGATION. Given the dynamic and multi-layered nature of VIP exposure at public gatherings, effective mitigation may require an integrated approach that combines physical security, coordination, and management of digital risk.

- Strengthen Multi-Entity Coordination
- Enhance Access Control Measures
- Limit Digital Exposure
- Incorporate Behavioral Detection
- Conduct Pre-Event Risk Assessments

Nihilistic Violent Extremists

Nihilistic Violent Extremism (NVE) is an emerging threat vector characterized by decentralized actors engaging in violence without coherent ideological alignment, instead motivated by grievance, nihilism, or a perceived need for recognition. The threat is enabled and accelerated by online ecosystems that facilitate recruitment, manipulation, and behavioral escalation.

For Faith-Based Organizations, NVE presents a different type of risk than traditional extremist threats. Rather than targeting organizations directly, it develops externally, most often in online environments, and surfaces through individuals connected to a community. This is particularly relevant for organizations with youth engagement or strong community ties.

Behavioral Drivers. NVE is defined less by ideology and more by underlying psychological and social drivers. Violence is often pursued as a form of identity construction or recognition, rather than to achieve a specific objective.

Engagement Pathways. Online platforms function as the primary operational layer for NVE activity. Engagement is typically gradual and structured to normalize harmful behavior over time.

Law enforcement reporting highlights targeted grooming of minors and vulnerable individuals, often through manipulation and coercion. Observed pathways are:

- Incremental exposure to harmful or violent content
- Reinforcement through peer validation and group belonging
- Escalation through coercion, including threats or blackmail

These pathways often lack clear transition points, complicating early detection.

Forward Trajectory. NVE ecosystems are adaptive and continue to evolve alongside digital culture. Research indicates increasing use of memes, gamification, and layered communication strategies to sustain engagement.

MITIGATION. Given the diffuse, behavior-driven nature of NVE and reliance on online ecosystems, mitigation requires a broader approach that emphasizes early identification, community awareness, and integration of non-traditional threat indicators into existing security frameworks.

- Prioritize Behavioral Indicators
- Enhance Digital Awareness
- Strengthen Early Detection
- Leverage Reporting Channels
- Account for Convergence Risks

Spotlight: More FB-ISAO Education Sessions

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 how 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!