

TLP CLEAR – IN OBSCURA CAVEATS APPLY



**(TLP-C) THREAT WARNING US OPERATION MIDNIGHT FURY - LION ROAR 28 FEB 2026
THREAT WARNING CONTINENTAL UNITED STATES**

###

**(CHRISTIANS, CHURCHES, CONGREGATIONS, ASSETS, PROPETIES, MISSIONARIES
FOREIGN (TELEGRAPHIC DISSEMINATION EXPEDITE)) 28 FEB 2026**

**CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED
UNCLASSIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND
ACTIONS DEEMED APPROPRIATE.**

CHURCH THREAT LEVEL – URGENT

DATE OF ACQUISITION: 28 FEB 2026

PUBLISHED: 28 FEB 2026

COLLECTION PERIOD: MARCH 2025 – 28 FEB 2026

INFORMATION CUTOFF: 28 FEB 2026

DISSEMINATION CONTROL: TRAFFIC LIGHT PROTOCOL-CLEAR (TLP-C)

PREPARED BY: V.M. NASTI

POINT OF CONTACT: V.M. NASTI

EXECUTIVE SUMMARY

THIS WARNING IS INTENTIONALLY BRIEF IN CONTENT

This Threat Warning issued upon execution of cited joint US/ISR tactical operations against targets inside the Islamic Republic of Iran about 0600 GMT (0100 NYC).

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN
OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies.
Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN
OBCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – IN OBSCURA CAVEATS APPLY

WARNING

FLUID, INCESSANT PRAYER

Based on a substantive body of open-source reporting, news media, US Government agency, firmly and tenaciously documented IN OBSCURA reporting active professional experience and depth: Churches MUST escalate and intensify proactive surveillance in securing their facilities, congregations, clergy.

Adding to this threat are the concurrent Ramadan, Christian and Jewish high holy days. Aggravated by recent unclassified disclosures of AT LEAST 18,000 Known or Suspected Terrorists were permitted to covertly infiltrate the US interior. This does not include the largesse of other similar operations, including discoveries of suspected WMD laboratories and foreign cartel street gang operations, and lastly the tactical environment in Mexico.

The Government of Iran has warned repeatedly of clandestine and covert cells it will activate inside the US if Iran is attacked. Note the Red Green Alliance IN OSCURA has provided reporting and warning. This axis is the current insurgency operating in our country. With HIGH confidence and on-going open-source collection and analysis, IN OBSCURA has warned the targeting of churches for attack.

CONTEXT

IN OBSCURA has since its inception, and several years prior to this as the former director of church security, warned repeatedly and tenaciously of the serious and escalating threat to Christians globally but more pointedly in the U.S.

The axis powers of the Red Green Alliance and its mutual aid aligned groups are controlled along with proxy groups inside the US. As well, elected US officials are have recently called for church attacks to escalate. As part of these Indications and Warning are numerous caveats and warnings of Islamist enemy attacks in Christian Genocide and those specific to US based Christians, that there would be retaliatory attacks inside the United States. Myriad IN OBSCURA raw and analysis products have repeatedly warned in writing with HIGH CONFIDENCE of Hybrid operations:

- Roe v Wade Reversal. Attacks and related operational activities in furtherance against targeted churches, clergy and pregnancy counseling centers. Inflammatory rhetoric

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – IN OBSCURA CAVEATS APPLY

which has intentionally sent command and signal messaging to attack and harass (persecute). The largesse of exploiting the First Amendment by elected officials, actors, anarchists, activists in furtherance and justification of kinetic action we have seen and is escalating.

- Target Surveillance. Inclusive of the Roe v. Wade kinetic attacks and continuing, personal witnessing and reporting of target intelligence collection of my church, police reporting. In IN OBSCURA monitoring of open sources, aggressively, since has indicated - based on professional acumen, prior to retirement. Massive target intelligence operations of churches and as of late, revival ministry for intended future attacks. This includes probable church computer penetrations and exfiltration of personally identifiable information on US Christians and Clergy.
- Escalation. Historic IN OBCURA threat warnings have emphasized repeated attacks and attempts. Within the last 90 days, dissemination SIGNIFICANT ACTIVITIES reporting (AKA IN OBSCURA NEWS Weekly) has emphasized the growing threats. The attack on the Cities Church in St. Paul to the attack in Meridian, Idaho and operations related are expanding the insurgency attacks on ICE. The calls by these insurgents AND elected officials inflammatory verbal targeting for MORE future church attacks should have been enough notice for Clergy.

=====DISSEMINATION=====

IN OBSCURA HAS ADOPTED THE OSINT CLASSIFICATION SYSTEM OF DEPARTMENT OF HOMELAND SECURITY CLASSIFICATIONS 'TRAFFIC LIGHT PROTOCOL' RELEASE CAVEATS. THESE REGULATE IN OBSCURA REQUIREMENTS FOR PUBLIC RELEASE TO PROTECT CLIENTS AND IN OBSCURA SOURCES, METHODS, AND TECHNIQUES. IN OBSCURA RELEASE PROHIBITION MARKINGS ALSO APPLY. NONE ARE RELEASABLE TO NEWS MEDIA OR JOURNALISTS WITHOUT WRITTEN REQUEST AND PERMISSION.

=====

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN OBSCURA PRODUCTS OR INFORMATION. TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION FOLLOW...

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

TLP CLEAR – IN OBSCURA CAVEATS APPLY

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 <p>TLP:RED For the eyes and ears of individual recipients only, no further disclosure.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.</p>	<p>Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.</p>
 <p>TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.</p>
 <p>TLP:GREEN Limited disclosure, recipients can spread this within their community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.</p>
 <p>TLP: CLEAR Recipients can spread this to the world, there is no limit on disclosure.</p>	<p>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.</p>

///END OF REPORT///

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY