

TLP CLEAR – DISSEMINATION UNLIMITED



(TLP-C) UPDATED SYNAGOGUE (2) ATTEMPT INFILTRATIONS, IVO BALTIMORE 19 June
2026 (UPDATED 20 JUN 2026)

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED

1 Chronicles 16:21-23

²² “Touch not Mine anointed and do My prophets no harm.”

²³ Sing unto the Lord, all the earth; show forth from day to day His salvation.

IN OBSCURA THEAT LEVEL – IMMINENT

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.

IMMEDIATE ACTION

Clergy, Church and Synagogue Security are to take this raw intelligence quoted below exceptionally seriously and take appropriate increased security countermeasures. This at a baseline means increased surveillance and detecting surveillance of your properties, related facilities, planned events and travel. Clergy and Security are advised to increase surveillance of your residences. Summer is the time for travel to foreign churches and missionaries, vacation bible school and weekly child-care at churches and synagogues. Expect the unexpected. Watch for anomalies. In this report it is noted that children in the congregation provided security access codes to the suspected hostiles.

IN OBSCURA COMMENT

FLASH Traffic means rapid dissemination of brief yet sufficient and actionable as indications and warning to all clergy, staff and security elements. Usually this is raw intelligence, not further elaborated at dissemination. It is likely this report below was hostile contact, because it would not be reported if this was legitimate contact. In the Intel, CT world this is considered **unsolicited** contact. These supposed police officers show up unannounced wearing odd uniforms at two different synagogues. Contact is first

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

TLP CLEAR – DISSEMINATION UNLIMITED

made with members of the congregation at each. Later they wore uniforms. No further information on details of how this occurred. The reported manner of contact suggest potential feigned urgency by the SUBJECTS.

It is further noted that the congregation members took appropriate action, possibly denying access to these targets. Kemp Mills is a named region of the urban suburb of Montgomery County, Maryland. It also has its own large police department. It is also home to several thousand Jews as a bedroom community of the Washington DC metro area. That this team was wearing uniforms is concerning, which is an anomaly and mandatory Suspicious Activity Reporting by US Government definition. This report was disseminated by a very close colleague who is a synagogue security and retired intelligence professional. The report is a copy of an alert message by the Community Security Service, a Jewish faith security organization...

IN OBSCURA EMPHASIS IS YELLOW BOLDED HIGHLIGHTED

(QUOTE) SITREP ALERT for 19 June 2026 – Possible New Adversarial TTP

Noted in the 19 June 2026 security brief from the Community Security Service:

Two White men, between the ages of 16-20, identified themselves as "Kemp Mill Peace Officers", and approached a congregant **near** a synagogue, **demanding** the synagogue's access code and **questioning** his religious identity. **That same evening**, the individuals **reportedly wore uniforms** with an **"ALTA" insignia, outside a different congregation and gained the access codes from children.** CSS Volunteers - Kemp Mill, Maryland (Tuesday - 6/9/26)

Should a similar situation occur while you are on post, DO NOT ALLOW ENTRANCE TO THE BUILDING. Procure the individual's (or individuals) credentials (Business Card, Operational Orders) and contact the issuing agency to certify their credibility.

Ask the agency to supply the name(s) of the individual(s) sent to your site. DO NOT give the name(s) of the individual (or individuals) at your door. The issuing agency should know who they sent to your site. Confirm with the name(s) on the individual's (or individuals) business card(s). Note any hint of deception on the part of the agency as the "agency" may be a person in collusion with the possible scam.

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

TLP CLEAR – DISSEMINATION UNLIMITED

If in question, call the local PD. Advise them of the situation. Ask if they had heard of the agency in question. Request a PD officer to your location if necessary. Do Not Allow Entrance to individual(s) waiting outside until thoroughly verified.

“But if the watchman sees the sword coming and does not blow the trumpet to warn the people and the sword comes and takes someone’s life, that person’s life will be lost because of the watchman’s sin.” – Ezekiel 33:6 (END QUOTE)

///END///

=====

REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN OBSCURA PRODUCTS OR INFORMATION.

TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 TLP:RED For the eyes and ears of individual recipients only, no further disclosure.	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.	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.
 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.	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.	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.
 TLP: GREEN Limited disclosure, recipients can spread this within their community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	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.
 TLP: CLEAR Recipients can spread this to the world, there is no limit on disclosure.	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.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

///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