In Obscura
Vincent M. Nasti, Founder, Chief Executive Officer, Consultant
In Obscura, LLC | Threat Intelligence | Security Countermeasures | Investigations
https://inobscura.org/

TLP-C IED DISCOVERY UNDERWATER, WATER RESEVOIR, MOBILE ALABAMA
KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED
IN OBSCURA THEAT LEVEL – IMMINENT

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

Explosive device found, detonated at Mobile water reservoir
Multi-agency team safely removed grenade-type IED discovered by divers at Converse Reservoir dam, By Robert Ristaneo, Fox 10, Published: May 13, 2026, at 5:52 PM EDT
https://www.fox10tv.com/2026/05/13/explosive-device-found-detonated-mobile-water-reservoir/

MOBILE, Ala. (WALA) - The Gulf Coast Regional Maritime Response and Render-Safe Team retrieved and detonated an improvised explosive device found underwater at the Converse Reservoir dam, the Mobile Area Water and Sewer System announced Tuesday. The multi-agency effort included the Mobile County Sheriff's Office, FBI Bomb Squad, Mobile Police Department Explosive Ordinance Detail, ALEA Bomb Squad and the Daphne Search and Rescue Team.

Divers surveying the dam for routine repair and maintenance located the grenade-type IED. MAWSS alerted the Mobile County Sheriff's Office, which coordinated the multi-agency response for analysis, retrieval, and safe demolition. "Our top priority is keeping your drinking water safe," said Bud McCrory, MAWSS director. **"This is an unprecedented threat,** and we are fortunate that this device was discovered before it could cause serious damage to our water supply or harm to individuals.

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

We are grateful for the professionalism and competency of our law enforcement partners – as well as the quick thinking of our contractors and divers – in identifying this device and safely destroying it."

ANALYST COMMENT

This is a significant event affecting national security, that of Defense and Commercial Critical Infrastructure[1]. The press release cites a "grade type device" ambiguous as it is, this is a potential attack threat until adequately defined by the authorities when prudent. There have been numerous open source media releases over several years concerning the threats to critical infrastructure, including detected surveillance, and suspicious persons reporting across the country. During April 2026, the US Environment Protection Agency released a threat reporting and cyber targeting alert[2] The threat environment continues to become complex and multi-faceted.

Churches are implored to be highly proactive and vigilant to detect and investigate suspicious activities and people. Specifically, highly recommended training is located here (Bombing Prevention, Bomb Threats, Suspicious Activity and Items, IED Awareness, Protective Measures Planning and Preparedness):

Suspicious Activity and Items

Learn how to recognize unusual behaviors and suspicious items typically associated with Improvised Explosive Device (IED) threats.

https://www.cisa.gov/topics/physical-security/bombing-prevention/suspicious-activity-and-items

[1] Dams Sector, The Dams Sector delivers critical water retention and control services in the U.S., supporting multiple critical infrastructure sectors and industries, US Cyber Security and Infrastructure Agency (CISA) https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/dams-sector

[2] Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure Publication: April 7, 2026, Federal Bureau of Investigation Cybersecurity and Infrastructure Security Agency National Security Agency Environmental Protection Agency Department of Energy United States Cyber Command – Cyber National Mission Force, https://www.ic3.gov/CSA/2026/260407.pdf

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

IED Awareness

Explore general Improvised Explosive Device (IED) and bombing prevention awareness information.

https://www.cisa.gov/topics/physical-security/bombing-prevention/ied-awareness

IN OBSCURA PRIOR REPORTING

TLP-C TACTCIAL INTELLIGENCE ANALYSIS 2023 MULTIPLE INTERSTATE CHURCH HOAX IED ATTACKS AND TARGET SURVEILLANCE OPERATIONS | REPORT DATE 4 FEB 2026

https://inobscura.org/tlp-c-tactcial-intelligence-analysis-2023-multiple-interstate-church-hoax-ied-attacks-and-target-surveillance-operations-report-date-4-feb-2026/

NOTE: This is a complex, multiple churches by the emplacement of hoax IED units across multiple US states. This occurred prior to the founding of In Obscura, LLC. This is a VITAL report and must be reviewed by church security professionals and clergy. Included is a copy of the JTTF Criminal Complaint which brings a detailed reality of what could have been a massive disaster.

TLP-C ///UPDATED///FLASH MESSAGE MULTIPLE IED DISCOVERY FT WASHINGTON PARK MD 23 MAR 26

https://inobscura.org/tlp-c-flash-message-multiple-ied-discovery-ft-washington-park-md-23-mar-26/

NEUTRALIZED IED ATTACK ANALYSIS (FINAL) CATHEDAL OF SAINT MATTHEW THE APOSTLE, 1725 RHIODE ISLAND AVE. NW, WASHINGTON DC, 2003

https://inobscura.org/wp-content/uploads/2025/10/NEUTRALIZED-IED-ATTACK-ANALYSIS-FINAL-ST-MATTHEWS.pdf

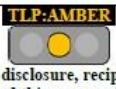
///END///

==========

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

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

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 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.
 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.
 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.
 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 OBCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA