

OFFICE of  
PRIVATE SECTOR

Liaison Information Report

**CROSS-SECTOR**

10 October 2023

LIR 231010002

**Public Safety Notification Regarding the Situation in Israel**

*References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.*

The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) are issuing this notification to advise of an ongoing issue of potential public safety concern consequent to the HAMAS attacks in Israel. The FBI and DHS are actively monitoring the situation in Israel and any implications these horrific terrorist attacks pose to the domestic threat environment. As with any potential threats to the United States, we will coordinate with our partners to ensure they have the resources and information necessary to keep our communities safe.

While we continue to collect and analyze intelligence from a variety of sources, we do not currently have specific intelligence reflecting additional attack planning against the United States stemming from the HAMAS attacks in Israel which began on October 7, 2023. However, as we have previously noted, foreign terrorist organizations and their supporters remain committed to attacking the United States within and beyond our borders. In recent years, there have been several events and incidents in the United States that were purportedly motivated, at least in part, by the conflict between Israel and HAMAS. These have included the targeting of individuals, houses of worship, and institutions associated with the Jewish and Muslim faiths with acts of physical assault, vandalism, or harassment.

Anti-Semitism permeates many violent extremist ideologies and serves as a primary driver for attacks by a diverse set of violent extremists who pose a persistent threat to Jewish communities and institutions in the United States and abroad. Foreign terrorist organizations have exploited previous conflicts between Israel and HAMAS via media outlets and online communications to call on their supporters located in the United States to conduct attacks. Some violent extremists have used times of heightened tensions to incite violence against religious minorities, targeting both Jewish and Muslim Americans.

**Available Resources**





The FBI and DHS encourage the public to promptly report information concerning suspicious activity to [tips.fbi.gov](https://tips.fbi.gov) or contact their local FBI field office ([www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices)). Call 911 to report emergencies, including imminent threats to life.

For concerns involving US citizens abroad, to include reporting missing persons or individuals taken as hostages, please call the Department of State's Overseas Citizens Services (OCS) toll-free hotline at (888) 407-4747 or complete Crisis Intake Form at <https://cacms.state.gov/s/crisis-intake>.



The FBI's Office of the Private Sector disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>.

**Traffic Light Protocol (TLP) Definitions**

<b>Color</b>	<b>When should it be used?</b>	<b>How may it be shared?</b>
<p><b>TLP:RED</b></p>  <p>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><b>TLP:AMBER</b></p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that <b>TLP:AMBER+STRICT</b> 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 <b>only</b>, they must specify TLP:AMBER+STRICT.</p>
<p><b>TLP:GREEN</b></p>  <p>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><b>TLP:CLEAR</b></p>  <p>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>