



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



PUBLIC HEALTH SECTOR

20 April 2020

LIR 200420-007

Threat Actors Exploitation of COVID-19 Pandemic Increased Threats to Medical Facilities

The FBI's Weapons of Mass Destruction Directorate in coordination with the Office of Private Sector is providing this LIR to inform state and local government first responders and public healthcare professionals of potential increased threats to medical facilities. The FBI is issuing this report due to recent incidents in which a racially motivated violent extremist (RMVE) targeted a medical facility and the Islamic State of Iraq in ash-Sham (ISIS) endorsement of attacks in countries impacted by the coronavirus disease 2019 (COVID-19). These incidents, as well as other RMVEs and other social media users advocating for violence against critical infrastructure, religious centers, and minority communities in response to the COVID-19 outbreak may entice violent extremists to target medical facilities.

- On 24 March 2020, FBI Kansas City disrupted a plan by a lone actor to attack a medical center using a vehicle-borne improvised explosive device in furtherance of the subject's domestic racially motivated violent extremist ideology. The perpetrator was a racially motivated violent extremist who wanted to attack the medical center because of the ongoing coronavirus pandemic and the increased media attention the attack would gain due to the target being a healthcare facility. ISIS' declaration for supporters to exploit the COVID-19 pandemic and conduct attacks.
- On 19 March 2020, ISIS issued its weekly *al-Naba* newsletter urged supporters to attack healthcare systems in Western countries that are strained by the COVID-19 pandemic.
- From February to April 2020, online posts by RMVEs and other social media users have advocated for violence against critical infrastructure and faith-based and minority communities in response to the COVID-19 outbreak.

Potential Threat Indicators:

The following list of indicators is advisory in nature and can be utilized by law enforcement and first responders to identify and mitigate potential threats. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

- Individuals surveilling medical facilities,
- Frequent, multiple perimeter surveillance 'false' alarms,
- Testing security; sabotage or holes in fences or security barriers,
- Vandalism of perimeter security equipment,
- Persons seeking employment who do not have proper identification documents, and
- Negligent professional behavior or abnormal individual personal behavior.



OFFICE *of* PRIVATE SECTOR





LIAISON INFORMATION REPORT (LIR)



This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your local FBI Weapons of Mass Destruction Coordinator and/or FBI Private Sector Coordinator at your [local FBI Field Office: https://www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices) or by calling 1-855-TELL-FBI.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.</p>