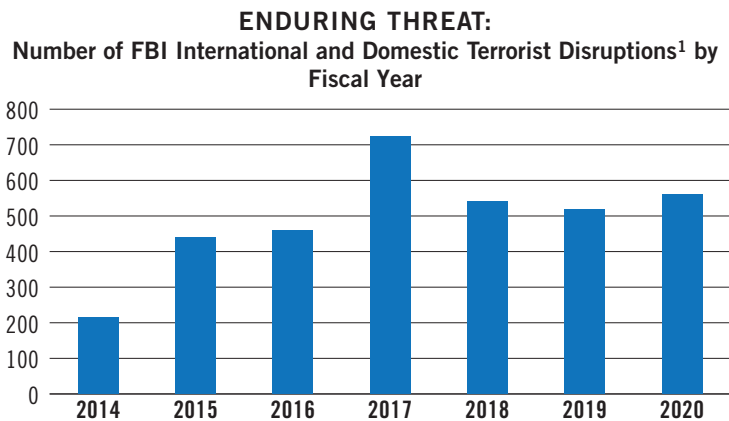


## Post 9/11 Response Evolution to an Enduring Threat

In the 20 years since the 9/11 terrorist attacks, incident prevention, disruption, and mitigation strategies have continued to evolve, impacting more than 2 million first responders. Information sharing, community outreach, and integration of intelligence into law enforcement's strategic and operational response plans are cornerstones of this effort. Asymmetrical terrorist threats require a tremendous commitment from the first responder community to evaluate and change traditional practices as needed and to ensure training, tactics, and operational procedures effectively and lawfully counter these threats.

**SCOPE:** This product provides awareness on evolving prevention, disruption, and mitigation strategies since 9/11.

**THREAT ENVIRONMENT:** The violent extremist threat emanating from foreign terrorist organization (FTO)-linked individuals in the United States has evolved from one defined by complex, large-scale attacks directed by an FTO to mostly self-initiated attacks by violent extremists inspired by an FTO and using relatively simple methods. Since 9/11 there have been three FTO-directed attacks in the US. Most attacks were perpetrated by US citizens inspired by ISIS or al-Qa'ida.



**MOBILIZATION INDICATORS AND SUSPICIOUS INCIDENT REPORTING:** Terrorists remain focused on conducting attacks, challenging first responders to hone their threat awareness while striving to adopt the tactics, techniques, and procedures (TTPs) necessary to ensure public safety and prevent terrorism. Fire, emergency services, and law enforcement personnel also continue to enhance their communications, coordination, operations, planning, and training to improve the survivability of victims and the safety of first responders in an increasingly complicated threat environment. This evolution in procedures and processes—combined with first responder awareness—has improved the critical response to incidents, as well as efforts to detect, deter, and disrupt potential terrorist attacks. The first responder community has made numerous operational changes since 9/11, resulting in the following protocols:

<sup>1</sup> According to the US Department of Justice Annual Performance Report, a disruption is defined as interrupting or inhibiting an international or domestic terrorist threat actor from engaging in criminal or national security related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest; seizure of assets; or impairing the operational capabilities of key threat actors.

**NOTICE:** This is a Joint Counterterrorism Assessment Team (JCAT) publication. JCAT is a collaboration by the NCTC, DHS and FBI to improve information sharing among federal, state, local, tribal, territorial governments and private sector partners, in the interest of enhancing public safety. This product is **NOT** in response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to terrorist tactics, techniques and procedures, whether domestic or overseas. Consider the enclosed information within existing laws, regulations, authorities, agreements, policies or procedures. For additional information, contact us at [JCAT@NCTC.GOV](mailto:JCAT@NCTC.GOV).



## Post 9/11 Response Evolution to an Enduring Threat *(continued)*

### Exercises and Training

- Develop and share best practices with federal, state, and local partners through interagency exercises and specialized training that is conducted at alternate locations, incorporates multiple scenarios (luring and secondary attack), and is put into practice as feasible.
- Conduct regular training on radicalization, mobilization towards violence, terrorist messaging, recruitment, and TTPs.
- Leverage training and resources available from interagency and intergovernmental partners.
- Become familiar with terrorist communication methods and platforms, TTPs, and messaging, to include instructions on how to make explosives and weapons.

### Investigations and Response

- Enhance investigative efforts in the Homeland involving domestic terrorism, homegrown violent extremism, and international terrorism through collaboration across jurisdictions.
- Conduct training on FTOs such as ISIS, and provide training on how to identify US persons traveling or attempting to travel overseas to fight on behalf of FTOs.
- Identify potential behaviors and indicators of radicalization or mobilization to violence during calls to service.
- Implement and use suspicious-activity reporting mechanisms and processes.
- Become familiar with assigned jurisdictions, to include surrounding areas outside of your area of responsibility (AOR).
- Assess the scene and conduct routine security sweeps for secondary devices, while relaying relevant information to responding agencies and jurisdictions.
- Conduct controlled field interviews and surveillance. For instance, do not meet alone with informants and avoid placing cover units in high-risk locations.
- Perform thorough screening of persons (informants or the general public) entering law enforcement facilities.
- Incorporate use of the Internet, electronic communication applications, and other social media platforms in terrorism investigations.
- Establish policies and procedures on bulk communication collections to strengthen the protection of individual civil liberties.
- Become familiar with terrorists' use of encrypted communications and the dark web.

### Collaborative Relationships and Information Sharing

- Establish working relationships with federal, state, local partners—to include NCTC, DHS, state and local fusion centers, and FBI Joint Terrorism Task Forces (JTTFs).



## Post 9/11 Response Evolution to an Enduring Threat *(continued)*

- Improve relationships with the community and private sector partners, to include technology companies, to aid in terrorism prevention efforts.
- Improve information-sharing efforts, to include incorporating the mention of counterterrorism (CT) intelligence products into briefings and roll calls, as well as with external partners.
- Promote interagency cooperation through agreements and protocols that clearly articulate the responsibilities of all participating agencies, with respect to resources, information sharing and services.
- Establish primary and alternative methods of communication through various federal, state, and local mutual aid agreements, as well as interaction with the private sector.
- Become familiar with internal and external control points and systems.
- Identify capabilities, roles, and responsibilities of key partners (medical services, private sectors, and security personnel).
- Coordinate, develop, and review mutual aid agreements and medical staging locations.
- Identify staging and treatment areas free of obstructions (dumpsters, flowerpots, trash cans, or vegetation), which may conceal secondary IEDs.
- Ensure evacuation plans result from close coordination, communication, and cooperation among all stakeholders and address venue activation, staging and mobilization of specified areas and personnel; location, traffic patterns, and egress points from premises and surrounding areas.
- Understand that emergency operations centers and dispatchers may be best positioned to identify luring, diversionary, or swatting tactics early because they have a collective operational picture of calls to service and anticipated response times throughout their respective jurisdictions and AOR.



## Post 9/11 Response Evolution to an Enduring Threat *(continued)*

### RESOURCES

#### DHS

- **Homeland Security Information Network** is a national, secure, and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, and private sector partners engaged in the homeland security mission. <https://hsin.dhs.gov>
- **If You See Something, Say Something®** is a program designed to raise public awareness of indicators of terrorism and terrorism-related crime and emphasizes the importance of reporting suspicious activity to the proper state and local law enforcement officials. <https://www.dhs.gov/see-something-say-something>
- **Nationwide Suspicious Activity Reporting (SAR) Initiative** helps to establish a nationwide capability for gathering, documenting, processing, analyzing, and sharing information on suspicious activities. <https://nsi.ncirc.gov/>
- **State and Local Fusion Centers** are focal points for the receipt, analysis, gathering, and sharing of threat-related information. <https://www.dhs.gov/fusion-centers>
- **Technical Resource for Incident Prevention (TRIPwire)** is a secure, online, collaborative information-sharing and resource portal for federal, state, local, and tribal government security and emergency services professionals. <https://tripwire.dhs.gov>

#### FBI

- **eGUARDIAN** is a repository of SAR accessible by law enforcement personnel and analysts directly supporting law enforcement. <https://fbi.gov/resources/law-enforcement/eguardian>
- **JTTFs** comprised of US law enforcement and intelligence agencies, who work together and use participating agencies' resources to preempt, deter, and investigate terrorism and related illicit activities. <http://www.fbi.gov/contact-us/field>
- **Law Enforcement Enterprise Portal** is a secure, Internet-based information-sharing system for agencies involved in law enforcement, first response, criminal justice, CT, and intelligence. <https://www.cjis.gov/CJISEAI/EAIController>
- **Terrorism Online Tips:** <https://tips.fbi.gov/>
- **Threat Screening Center** provides information, training, and resources. <https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc/tsc>

#### NCTC

- **Homegrown Violent Extremist Mobilization Indicators for Public Safety Personnel - 2019 Edition** identifies behaviors that indicate an individual or group may be preparing to engage in violent extremist activities and is available on the ODNI website. <http://go.usa.gov/xEKgd>

#### OTHER

- **Legal Changes to Enhance CT Efforts** <https://www.justice.gov/archive/911/legal.html>
- **USA Freedom Act** was developed to reform the authorities of the Federal Government so that it may require the provision of certain business records, conduct electronic surveillance, use pen registers and trap-and-trace devices, and use other forms of information gathering for foreign intelligence, CT, and criminal and other purposes. <https://www.congress.gov/bill/114th-congress/house-bill/2048/text>
- **USA Patriot Act (2001)** was developed to deter and punish terrorist acts in the US and around the world, to enhance law enforcement investigation tools, and for other purposes. <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>





## PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE:    LE    FIRE    EMS    HEALTH    ANALYSIS    PRIVATE SECTOR    DATE:

PRODUCT TITLE:



ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

