US Elections: Violent Extremists Threat Environment Considerations for the Public Safety Community

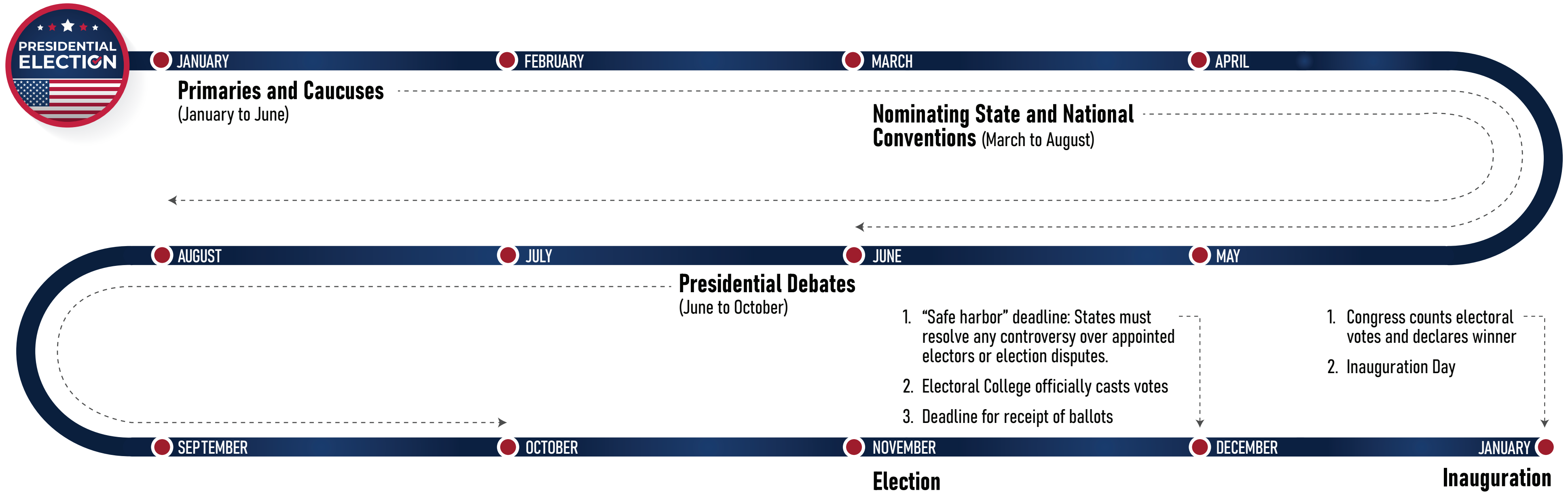
SCOPE: This product offers considerations for election security partners, first responders, the private sector, and other officials to help identify, prevent, and respond to violent extremist threats against the US electoral process. This product is not a response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to international terrorism threats and/or threats resulting from general terrorist tactics, techniques, and procedures. In this product, NCTC uses the term "violent extremists" to refer to foreign violent extremists and those US-based violent extremists who are directed, enabled, and inspired by, or who otherwise affiliate or collaborate with, foreign violent extremists.

Some violent extremists messages are aimed at encouraging threat actors to exploit the current US election cycle by sowing violent discord. These efforts may be aimed at exploiting the widespread media attention that election-related events garner and undermining public confidence in the United States' democratic process. Violent extremists influence through messaging efforts—coupled with the likelihood of a broad increase in election-related threat reporting in the preelection and postelection cycles—underscore unique public safety considerations for the first responder community.

- In July 2022, an identified transnational racially or ethnically motivated violent extremist publication encouraged individuals to promote narratives regarding perceptions of election fraud and corruption to undermine the legitimacy of the electoral system. The same publication stated that "real change" came through violence, not voting. It also encouraged attacks against government officials, minorities, other civilians, and critical infrastructure.
- In November 2016, ISIS released a seven-page English-language article that denounced Muslims in the United States for participating in democratic elections and urged US-based ISIS supporters to attack voters participating in the then-upcoming Presidential election. Also in 2016, al-Qa'ida threatened extremist violence against multiple states the day before the US general election, raising public safety concerns.
- In 2021, al-Qa'ida in the Arabian Peninsula (AQAP) released the sixth issue of *Inspire Guide* in English and Arabic, focusing on the attack at a Boulder, Colorado, supermarket that killed 10 people. The issue highlighted tactical recommendations for would-be attackers and amplified the impact of the event, citing "increased division between the American people, between the right and the left, and between the Republicans and their supporters, and the Democrats and their supporters." Also in 2021, AQAP released a 20-minute video with footage from the 6 January 2021 violent breach of the US Capitol. In the video, AQAP's leader stated that the "incident of breaking into the Congress [w]as only a little bit of what will happen to them [the United States]." Since December 2023, the group has also released two videos that promoted violence against public officials, including US persons.

Nominal Depiction of Presidential Election Cycle Events

The election cycle is a protracted and complex operating environment for the public safety community. The security footprint extends beyond election infrastructure and may include federal, state, local, government personnel and buildings, candidates, judicial figures associated with electoral challenges, private companies connected with vote counting, officials involved in counting certifications, and voters.



Primaries and Caucuses (January to June)

Nominating State and National Conventions (March to August)

Presidential Debates (June to October)

1. "Safe harbor" deadline: States must resolve any controversy over appointed electors or election disputes.
2. Electoral College officially casts votes
3. Deadline for receipt of ballots

1. Congress counts electoral votes and declares winner
2. Inauguration Day

Election

Inauguration

Resources

DHS

- **Cybersecurity and Infrastructure Security Agency (CISA) Election Security Trainings** provide additional guidance to election stakeholders in managing risk and strengthening election infrastructure resilience. To schedule or to learn more about these trainings, email: electionsecurity@hq.dhs.gov
- **CISA's Interagency Security Committee** provides training that may be useful to securing physical infrastructure during elections. www.cisa.gov/interagency-security-committee-training
- **CISA Election Security** https://www.cisa.gov/topics/election-security
    - **Election Infrastructure Insider Threat Mitigation Guide** https://www.cisa.gov/sites/default/files/2022-11/election_insider_threat_mitigation_guide_508_0.pdf
- **National Threat Evaluation and Reporting Program Office—Nationwide Suspicious Activity** https://www.dhs.gov/nationwide-sar-initiative-nsi

FBI

- **FBI Election Crimes and Security** provides information on reporting election-related crimes. www.fbi.gov/elections
- **FBI Tip Line** is FBI's hub for reporting election and nonelection threats and crimes. https://tips.fbi.gov or 1-800-CALL-FBI (225-5324)

Other

- **US Election Assistance Commission (EAC)** serves as a national clearinghouse for election administration. www.eac.gov/election-officials/election-security
- **CISA, FBI, US Postal Inspection Service (USPIS), EAC Election Mail Handling Procedures To Protect Against Hazardous Materials** https://www.cisa.gov/sites/default/files/2024-02/Election%20Mail%20Handling%20Procedures%20Joint%20Product_02.12.2024_V3_508c.pdf
- **CISA, DHS, DOJ, FBI, ODNI, USPIS Federal Executive Branch Agencies Roles and Responsibilities in United States Elections** https://www.dni.gov/files/ODNI/documents/assessments/Interagency_Election_Security_Fact_Sheet_022024.pdf
- **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)**[a] offers a suite of election security resources. www.cisecurity.org/ei-isac

[a] This resource is listed to illustrate the variety of offerings and is not to be considered endorsements of the content of the material or trainings offered.

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, the FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies or procedures. For additional information contact us at JCAT@ODNI.GOV. **This document is best printed in 11 X 17.**

NCTC-JFRT-2024-06275

28 MAY 2024
AUTHORED BY NCTC, DHS, FBI

CONSIDERATIONS

Understanding violent extremists' tactics, techniques, and procedures (TTPs) may enhance detection efforts, improve incident response, and broaden information sharing. The following considerations are offered for public safety officials, the private sector, and other homeland security partners to enhance awareness of efforts dedicated to identifying, protecting, mitigating, and responding to election security–related threats throughout the election cycle. Departments are encouraged to follow their agency policies, standard operating procedures, and established protocols when responding to potential threats.

Refer to the related First Responder's Toolboxes highlighted within each section for more detailed information, which can be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.

Tactics, Techniques, and Procedures

Violent extremists may use simple tactics and a range of easily accessible weapons to attack or threaten opportunistic targets or engage in violence against symbolic targets and perceived ideological opponents. Potential threats associated with election targets may increase given the amplified violent extremist messaging and discord. Public safety officials are encouraged to develop awareness of election-related infrastructure, personnel, and elements critical to elections, which may include political candidates, campaign headquarters and campaign-associated gatherings, state and local election offices, government personnel, ballot drop-box locations, voter registration sites, polling locations, postelection vote count and election certification facilities, and events surrounding inaugurations.

"Vehicle-Borne Attacks: Tactics and Mitigation," December 2020 | "Terrorist Messaging Urges Use of Edged Weapons," November 2020 | "Unmanned Aircraft System (UAS): Recognizing Malicious Modification," September 2020 | "IED Manufacturing Indicators," July 2019 | "Postal and Shipping: Identification and Mitigation of Suspicious Mail and Packages," November 2018 | "Complex Operating Environment—Attacks From Elevated Positions," November 2017 | "Terrorists Likely To Attack Opportunistic Targets Using Readily Available Weapons, Limiting Time for Detection and Disruption," May 2017 | "Recognizing Arson With a Nexus to Terrorism," April 2017

Insider Threats

Violent extremists may seek to use witting and/or unwitting trusted insiders[b] to gain authorized access to or special understanding of an organization and its processes. Procedures that deter, detect, and prevent harm by insider threats are an integral part of conducting secure elections. Election infrastructure partners may benefit from officially documenting their approaches and establishing formal insider threat mitigation programs, which can help identify gaps in current practices.

"Terrorist Insider Threat," September 2020

Physical Security

The electoral process, its infrastructure, and campaign-related activities consist of an array of preelection, election day, and postelection activities and events impacting federal, state, local, and private sector stakeholders. Many aspects of the electoral process prioritize public accessibility and require public safety officials to enhance security.

"Awareness of Violent Extremist Tactics to Defeat Physical Security Can Improve Response," September 2021 | "Complex Operating Environment—Special and Other Significant Events," August 2020 | "Planning and Preparedness Can Promote an Effective Response to a Terrorist Attack at Open-Access Events," March 2018 | "Complex Operating Environment—Hotel High Rise," November 2019

Identifying and Reporting Suspicious Activity

Public safety personnel and bystanders are uniquely positioned to report activities and behaviors associated with criminality, including activities and behaviors with a nexus to terrorism. Public safety personnel and bystanders may observe suspicious behaviors or activities throughout the protracted election cycle, including during interactions with the public, calls for service, or while conducting investigations.

"US Violent Extremist Mobilization Indicators Booklet," 2021 Edition | "Reporting Suspicious Activity—Critical for Terrorism Prevention," October 2022 | "Bystanders Are Key to Countering Terrorism," November 2020 | "Hospitality Industry: Enhanced Suspicious Activity Awareness Assists in Terrorism Prevention," November 2019

Lawful Public Assemblies

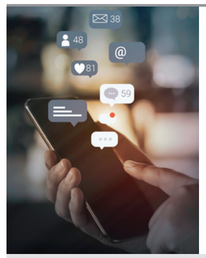
Lawful public assemblies[c] such as protests, rallies, and demonstrations[d] may stoke tensions between participants and perceived ideological opponents and present opportunities for violent extremists to exacerbate domestic divisions. Violent extremists may seek to inflame such tensions online, amplify messaging sympathetic to their causes, and disrupt election processes and First Amendment–protected activities through violent tactics and methods. Violence can occur with little to no warning. Some indicators of extremist violence may be observed during pre-event gathering and planning, while others will only be observable during actual events.

"Awareness of Violent Extremist Tactics to Defeat Physical Security Can Improve Response," September 2021 | "Violent Extremists and Terrorists Exploit Civil Unrest and Public Assemblies in the United States," July 2020

Public Figures and Government Facilities

Violent extremists may direct violence or threats at government or election-related officials, polling venues, voters, and campaign-related events. Identifiable features like uniforms and logos make potential targets highly visible, and the accessibility of government officials and public facilities create security challenges. Improved digital literacy may help protect against revealing details regarding patterns-of-life online or other sensitive details. Awareness of state laws regarding threats to officials may also help with response considerations.

"Protection Considerations for Violent Extremist Threats to Public Officials," February 2022 | "Personal Security of First Responders in the Digital Age," March 2021 | "Persistent Threat of Terrorist Ambush Attacks on First Responders," January 2020 | "Bus Attacks Highlight Potential Tactics and Mitigation Efforts," April 2019 | "Complex Operating Environment—Motorcades," November 2016



Influence[e] and Interference[f] Through Messaging

Violent extremists may try to amplify and disseminate narratives online that promote violence and aggravate social and political divisions. Such messaging might be geared at encouraging attacks against symbolic targets and/or perceived ideological opponents and undermining confidence in US democratic institutions. These efforts could contribute to individuals' self-radicalization and, in extreme situations, result in people undertaking violent responses to perceived grievances. Violent extremists may attempt further disruption through tactics such as sending white powder letters, hoax threats, or suspicious packages.

"Violent Extremists Likely Will Continue To Use Disinformation on Social Media Outlets To Instill Fear and Radicalize Others," August 2018 | "Postal and Shipping: Identification and Mitigation of Suspicious Mail and Packages," November 2018

Online Activity

Violent extremists may try to create, communicate, and distribute threats using an array of cyber tactics. These tactics may include spoofed emails, spear phishing, exploiting the vulnerabilities of US state election websites, denial of service attacks, and illegally registering website domain services in the United States—all aimed at broadening extremists' reach and access to sensitive information. Foreign terrorist organizations have tried to influence elections abroad and may employ similar tactics during the US election cycle. Advanced cyber tools provide violent extremists low-cost and scalable options and do not require physical access to targets.

"Violent Extremists' Use of Generative Artificial Intelligence," May 2024

[b] An *insider* is a current or former employee or person with regular access to a facility who provides information or materials.

[c] The US Constitution guarantees the right to peaceable public assembly and free speech.

[d] Although most violence during lawful public assemblies has been historically criminal in nature, and not associated with terrorism, some violent extremists perceive these events as opportunities to engage in violence.

[e] Overt and covert efforts to affect US elections either directly or indirectly.

[f] Subset of election influence activities targeted at technical aspects of elections, including voter registration, casting ballots, and counting ballots, or reporting results.

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, the FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies or procedures. For additional information contact us at JCAT@ODNI.GOV. **This document is best printed in 11 X 17.**

28 MAY 2024
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.