Enhancing Security for High-Profile Figures at Public Gatherings

SCOPE: This product provides state and local public safety officials and personal security details with considerations for identifying and mitigating potential terrorist threats at large public gatherings involving high-profile or influential figures (referred to as *VIPs* in this product).[a] Security for most public gatherings in the United States is managed at the state and local levels and does not involve Federal support. This product is not in response to a specific threat or ongoing plot in the Homeland. It was authored with contributions from the Scottsdale Police Department.

VIP attendance as a guest, speaker, or delegate at a large public gathering requires a flexible planning process. As new terrorist threats are detected, risk factors assessed, and protective factors or precipitating events identified, public- and private-sector partners should conduct threat assessments and proactively update their accompanying mitigation plans. Close partnerships between Federal partners, state and local public safety officials, venue staff and security, and private security details are key to identifying and mitigating potential terrorist threats.

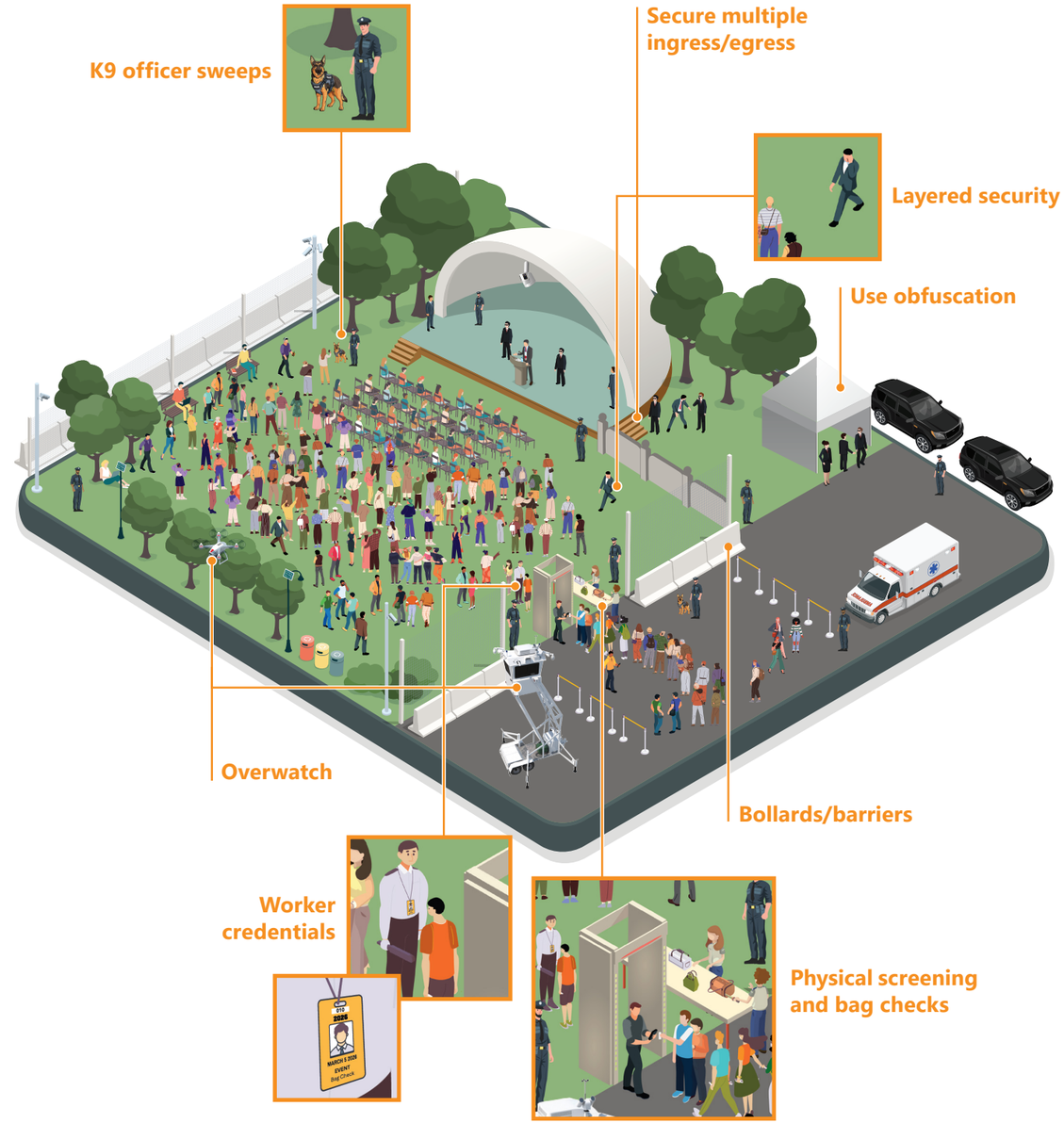
- An Iranian asset used a network of criminal associates he met in prison in the United States to surveil and plot the murder of a US citizen of Iranian origin who has been an outspoken critic of the Iranian regime. The individual's appearance at a northeastern university was canceled because of the ongoing surveillance and threats after the FBI shared pertinent details with the university.

Considerations

The following are considerations for public safety and private security that may be beneficial to incorporate in planning efforts. For additional information about terrorist tactics, techniques, and procedures and mitigation considerations, refer to the relevant First Responder's Toolboxes highlighted in the text boxes. These resources are available on JCAT's website, DHS's Homeland Security Information Network, and FBI's Law Enforcement Enterprise Portal.

Pre-Event Physical Security Coordination

- Effective and efficient physical security of VIPs is often relationship-based. Private security details should anticipate coordinating with event organizers, venue managers, and law enforcement partners to establish a security plan and conduct a site survey with the advance team. Collaboration can identify a secured venue that takes into account the dynamic threat environment.
- Identify a VIP's planned arrival and departure methods (blending in with the crowd or obfuscating movement through a separate tented or draped entrance), backup routes, and defined VIP areas (including private restrooms and elevators).
- Establish secure communications, including an emergency notification system for potential threats or emergency response protocols.
- Consider sharing state and local jurisdictional concerns and providing maps to help familiarize the security detail with the area.
- Determine ahead of time who within the state and local chain of command has authority to shut down the event in case of a public safety threat.



[a] These figures include but are not limited to activists, advocates, celebrities, cultural icons, business leaders, and entrepreneurs who have widespread recognition and may have far reaching-media coverage, significant social media presence, or cultural/socio/political influence or regularly attend public engagements.

NCTC-JFRT-2026-04758
30 MARCH 2026
AUTHORED BY NCTC, DHS, FBI

Enhancing Security for High-Profile Figures at Public Gatherings *(continued)*

Pre-Event Physical Security Coordination *(continued)*

- Encourage private security details to be certified in first aid and lifesaving skills, have a trauma kit on-site, know where the nearest advanced trauma centers are located, and have access to emergency phone numbers.
- Conduct physical risk and vulnerability assessments, evaluating the need for physical security like bollards, barriers, and CCTV.
- Maintain awareness of potential flashpoints for violence that may spill over or impact the security and response plan, like planned or spontaneous lawful public assemblies that may attract counterprotesters. Have a contingency plan with protocols for responding to unexpected threats or events.
- Conduct security sweeps and maintain security oversight of the venue and VIP bed-down locations before the event. Repeat checks, looking for changes to security posture, during the event.
- Consider how ongoing investigations and the changing threat landscape might intersect with public events in an agency's jurisdiction. Work with analytic support to identify key terms and phrases for detecting potential online threats.
- Submit a temporary flight restriction request to the Federal Aviation Administration (FAA) to limit malicious UAS operations during the event. Refer to the FAA's Public Safety Small Drone Playbook for more information about the difference between authorized and unauthorized UAS operations and potential public safety actions.

Complex Operating Environment—Special and Other Significant Events | *Protection Considerations for Violent Extremist Threats to Public Officials* | *Complex Operating Environment—Motorcades* | *Complex Operating Environment—Educational Facilities: Post-Secondary Institutions* | *Iran-Linked Lethal Operations in the United States*

Screening and Access

Events often require support from contractors, vendors, or volunteers, many of whom are hired temporarily or contracted through third-party organizations. In some cases, these personnel are hired informally or without thorough security screenings. Enhanced collaboration between public- and private-sector partners that includes a more rigorous security screening process can help protect from potential insider threats.

- Develop a standard procedure to determine appropriate background and security checks, organizational responsibilities for credentialing, and a process to document and report any derogatory findings.
- Limit unauthorized entry to sensitive or secure areas with access control measures, like event ticketing, badges, or wristbands, which can also generate tips or leads for investigative purposes. Other protective measures include metal detectors and bag checks that limit prohibited items from entering a facility.
- Clearly identify private security detail members who are authorized to carry weapons with specific credentials, badges, or wristbands. Security details should notify local law enforcement in charge of the event of their intention to bring permitted weapons onto the premises.
- Control the security credentialing process to limit the potential for counterfeiting, and use color-coding and protective features (for example, holograms and watermarks) to distinguish access levels and roles and to verify genuine credentials.
- Mix or layer direct hires, including law enforcement and third-party hires, among various security locations to limit vulnerabilities at particular sites.

Third-Party Security Critical to Safeguarding Public Gatherings From Terrorist Threats | *Evolving Landscape: Fraudulent Document Use To Circumvent Detection and Screening* | *Terrorist Insider Threat* | *Planning and Preparedness Can Promote an Effective Response to a Terrorist Attack at Open-Access Events*

Event Collaboration and Information Sharing

- Designate points of contact between venue staff and on-site security, law enforcement, and personal security details to ensure rapid communications in the event of a threat; enhanced relationships facilitate regular sharing of threat information or other security concerns. Boost information sharing through the state and local fusion centers' threat liaison officer programs and through the FBI's Joint Terrorism Task Forces.
- Establish a lead to contact and update the media with relevant information. Promote communication platforms (official websites or social media accounts) through which the public can report suspicious activity or tips and organizers can release information to the community in the event of an active response to a threat (such as a road closure or incident status).
- Use strategic positions around venues for law enforcement overlook activities before and during the event. Engage technical monitoring, like UAS, to assist with overwatch activities. Prepare a UAS launch and recovery area away from the target area. Test UAS command and control, communications, and video-streaming capabilities.
- Establish accountability measures and communication protocols across partners to ensure the range of security requests and incidents are followed up on and executed successfully.

Complex Operating Environment—Special and Other Significant Events | *Responses to Overseas Conflicts May Impact Public Safety Agencies in the Homeland*

Threat Assessment and Threat Management

- Encourage private security details to coordinate with state and local officials to develop a plan regarding individuals who may be exhibiting concerning behaviors on the pathway to violence, such as stalking or harassing. Assess risk factors that increase the likelihood of violence in a given situation; identify stabilizing or protective factors that could prevent the individual from conducting violence; and identify stressors and triggers—past, current, or anticipated events—that may build up over time.

Threat Assessment and Threat Management series

Digital Security

- Evaluate the threat environment and weigh the benefits of limiting the public release of specific information tied to personal and event security, including detailed event schedules, guest lists, attendee profiles, or other security details not required for public access to the venue. Highlighting event security requirements through public media campaigns may dissuade individuals from targeting the VIP or attempting to access the venue illicitly.

Personal Security of First Responders in the Digital Age | *Personal Security for First Responders* | *Evaluating and Responding to Violent Extremist Hoax Threats*

Resources

NCTC-DHS-FBI *US Violent Extremist Mobilization Indicators* booklet (2025)

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) online training

FAA Law Enforcement Assistance Program

NCTC-JFRT-2026-04758
30 MARCH 2026
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.