Third-Party Security Critical to Safeguarding Public Gatherings From Terrorist Threats

SCOPE: This product offers event planning considerations for public safety officials and other private-sector partners in light of potential terrorist plotting in the US. This product was authored with contributions from the Southern Nevada Counterterrorism Center.

Events often require temporary support from large numbers of employees, contractors, and volunteers, many of whom are hired temporarily or contracted through third-party and vendor organizations. Terrorists have demonstrated their intent to use insiders[a] with unique positions of access to facilitate and conduct attacks, enter secure areas, and obtain sensitive information to exploit the security processes and procedures of venues or host organizations. Informal hiring or screening practices for temporary workers may result in diminished ability to identify potential insider threats. Proactive operational and personal security considerations and suspicious activity reporting are key elements to protect public gatherings from potential insider threats. Collaborating in advance with private-sector partners to implement more rigorous security screening procedures is also important.

- In August 2024, Austrian authorities disrupted ISIS-inspired plotters intending to target the concert of a US person singer. One of the individuals connected to the plot was employed by the company responsible for providing security and logistic services at the concert venue.

Considerations

The following information may assist event planners and host organizations mitigate insider threats when hiring temporary workers and discussing third-party security services with public safety officials in support of events.

[a] An insider is a current or former employee, contractor, volunteer, or person with access to a facility and/or restricted data who provides information or materials intended to harm through malicious, complacent, or unintentional acts that affect the integrity, confidentiality, and availability of the organization, its data, personnel, facilities, and associated resources. Insiders may or may not actively participate in attacks.

NCTC-JFRT-2025-06421
15 APRIL 2025
AUTHORED BY NCTC, DHS, FBI

Security Screening

- Engage early in the event planning process with third-party security services to understand their current security screening standards and requirements.
- Develop standard operating procedures to determine appropriate background and security checks and organizational responsibilities for credentialing.
- Determine how to document and report findings in the event that derogatory information is found.
- Allow sufficient time during event planning discussions to accommodate for any security screening checks that the host organization may request.

Credentialing

- Standardize the type and level of credentials required for temporary workers and the protocols for receiving them.
- Regulate physical access to sensitive areas to essential personnel based on the roles and functions of particular positions.
- Determine if vehicle registration and credentialing is needed. Report and investigate potential misuse, theft, or loss of credentials and perform ID checks on each individual entering restricted areas.
- Limit the time between events and when security credentials are distributed to avoid the potential for counterfeiting.
- Destroy or deactivate credentials that are expired or otherwise no longer valid. Develop protocols for revoking credentials when necessary.
- Mix or layer direct hires and third-party hires within and among various security locations to limit vulnerabilities at particular sites.
- Employ photo identification, personal information, and protective features—like holograms and watermarks—and color coding to highlight access levels and roles, assist with identity verification, and prevent counterfeiting.

Threat Awareness

- Enhance information sharing among stakeholders by holding routine briefings, conducting regular engagements, and circulating timely threat reporting.
- Designate specific liaisons to coordinate information sharing with the lead public safety agencies responsible for security and providing all-hazards response capabilities.[b]
- Establish partnerships with local law enforcement and state or local fusion centers or FBI field offices to facilitate reporting of threat activity in a timely manner.

Training

- Provide comprehensive training to employees, contractors, and volunteers. Training should cover essential security practices, thresholds for reporting suspicious activities, and insider threat awareness.
- Require regular recurring (e.g., annual) training to reinforce the importance of security and actions to take in the event of incidents and attacks.
- Deliver training on how to identify and report suspicious activities, including insider threat and other terrorism-related behaviors, indicators of possible mobilization to violence, and behavioral threat detection training.
- Collaborate with relevant federal partners to apply their unique capabilities, training, and resources, especially during events and public gatherings.

Indicators of Suspicious Activity[c]**:** Security practitioners are encouraged to establish a baseline of suspicious activities at each location, jurisdiction, and venue. Some of the indicators listed below have been used in pre-operational activities by terrorists and violent extremists. Any atypical activity or behavior may be considered suspicious, including the following:

- Unusual or prolonged interest in the movements of VIPs, performers, and athletes, particularly in areas or assignments outside an employee's responsibilities;
- Improper use of information technology systems and repeated attempts to access restricted information or resources not associated with a person's role or position;
- Repeated attempts to enter restricted areas without proper credentials;
- Repeated breaches of rules, procedures, or policies without reasonable explanation;

[b] All-hazards approach is a capabilities-based approach to preparedness to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

[c] Behavior associated with these indicators may include constitutionally protected activities. Evaluating the totality of behavioral indicators and other relevant circumstances should be evaluated when considering any follow-up response or action. Do not initiate any investigative or intelligence activity based solely on the exercise of a constitutionally protected activity.

- Off-duty presence on the property, possibly accompanied by unknown or unauthorized individuals;
- Direct or implied threats or statements that indicate a potential desire to engage in violence;
- Inquiring or eliciting[d] information about, monitoring or recording security equipment, plans, procedures, movement, or responses without a reasonable explanation;
- Concealing the use of a camera or video camera, including taking photographs or videos of security cameras, loading docks, and ingress and egress points;
- Making notes, diagrams, or sketches of an area;
- Eliciting information about facilities or events (e.g., vulnerabilities) that are outside the scope of the employee's job without a reasonable explanation;
- Making observations of or asking questions about the HVAC (ventilation) systems of a facility; and
- Loitering in areas where work is no longer being performed by the individual.

[d] Elicitation often initially appears as being part of a routine social or professional conversation.

RESOURCES

THE NATIONAL THREAT EVALUATION AND REPORTING (NTER) PROGRAM OFFICE

https://www.dhs.gov/nter

- Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) eLearning Modules
  https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training
- Foundations of Targeted Violence eLearning Module
  https://www.dhs.gov/foundations-targeted-violence-prevention

STATE AND MAJOR URBAN AREA FUSION CENTERS

https://www.dhs.gov/fusion-center-locations-and-contact-information

FBI FIELD OFFICES

https://www.fbi.gov/contact-us/field-offices

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Public Venue Credentialing Guide

https://www.cisa.gov/resources-tools/resources/public-venues-credentialing-guide

Insider Threat Mitigation Guide

https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

DHS, FBI, NCTC

US Violent Extremist Mobilization Indicators Booklet (2021 Edition)

https://www.dni.gov/index.php/nctc-newsroom/nctc-resource s/3590-u-s-violent-extremist-mobilization-indicators-2021

NOTICES & HANDLING CAVEATS

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 product is not in response to a specific threat against the Homeland but is intended to provide background information and additional resources related to possible threats from foreign violent extremists; US-based violent extremists who are directed, enabled, or inspired by, or who otherwise affiliate or collaborate with foreign violent extremists; and general terrorist tactics, techniques, and procedures employed by such actors.

NCTC-JFRT-2025-06421
15 APRIL 2025
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.