

Protecting High-Profile and High-Risk Court Proceedings Against Terrorist Threats

SCOPE: This product provides an overview of security considerations to help public safety officials prepare for high-profile, high-risk court proceedings and secure them against terrorist threats. It was coauthored with members from the Orange County Intelligence Assessment Center, Los Angeles Joint Regional Intelligence Center, and the Supreme Court of the United States Police Department. Various jurisdictions may have different thresholds for determining what is a high-profile or high-risk case, requiring adjustments to the scale and scope of their actions based on local priorities and current events. The planning phase should consider protection for the entirety of the court system, including judges, clerks, facilities and maintenance, and information systems. This product is not a response to a specific terrorist threat. It is a resource for public safety officials responsible for identifying and mitigating such threats in their jurisdictions.



High-profile, high-risk court proceedings^a present complex planning and security challenges for court and public safety officials against terrorist threat actors. While acts of terrorism against court proceedings are infrequent in the United States, terrorists may attempt to target public officials, informants, and cooperating witnesses to retaliate, intimidate, or obstruct justice. Since US court proceedings are generally open to the public, enhanced security measures are sometimes necessary to mitigate potential threats to court staff, public safety officials, the jury, witnesses, court facilities, and the public, especially during high-profile or high-risk court proceedings.

The foreign terrorist organization-designated New Generation Jalisco Cartel (CJNG) and Sinaloa Cartel have conducted attacks against authorities in Mexico and, in some cases, killed sources and cooperating witnesses linked to the trials of senior cartel members. In 2024, members of the CJNG surveilled US Drug Enforcement Administration officials and witnesses in Washington, DC, during the trial of the son of CJNG's overall leader.

Considerations

High-profile, high-risk court proceedings are complex security environments that require coordinated and comprehensive security measures. The following information may help public safety and court officials prevent, mitigate, and respond to threats.

Information Sharing and Threat Awareness

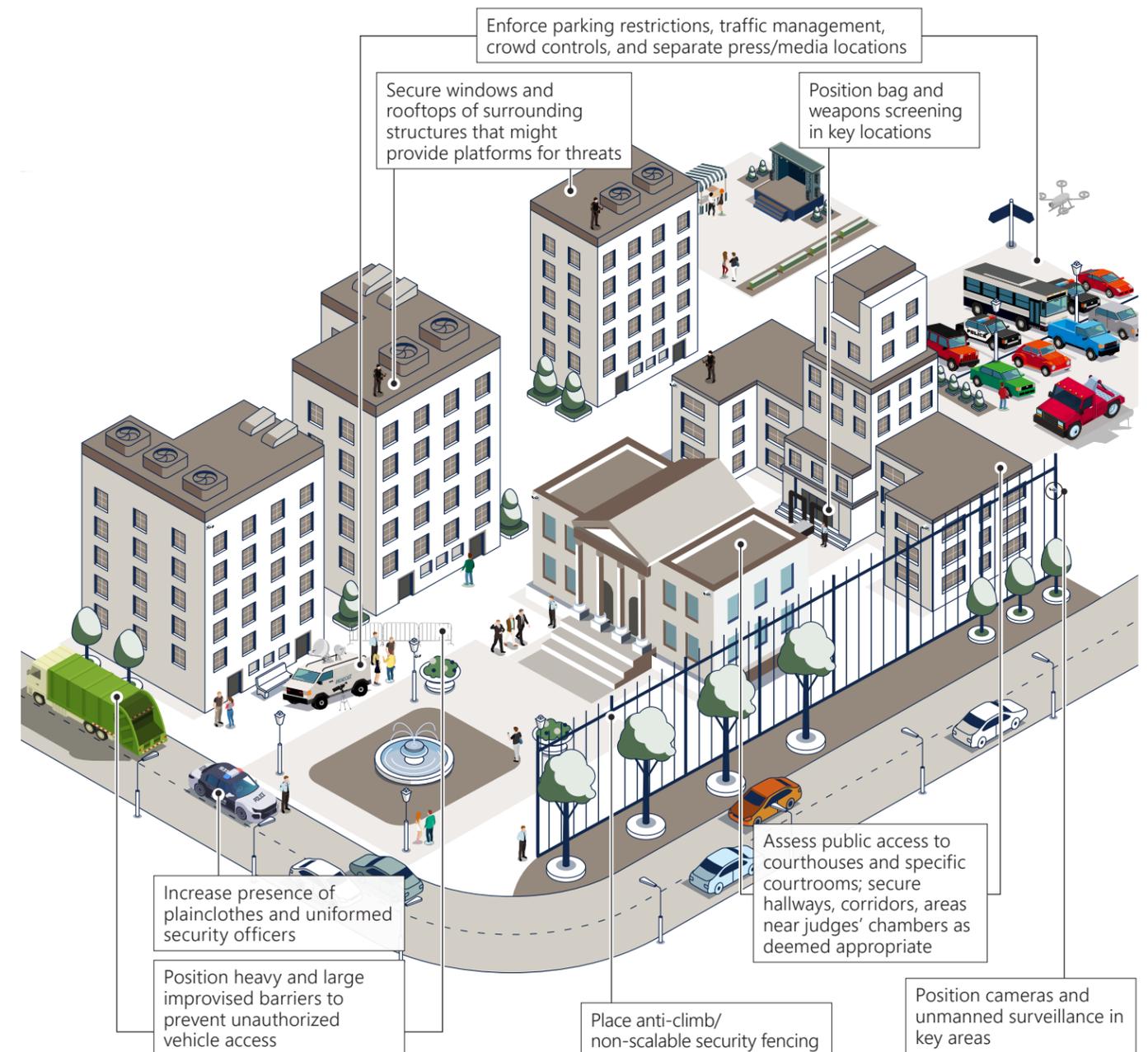
- Coordinate with federal partners such as the US Marshals Service, the US Federal Protective Service, and state and county judicial protection units. For cases linked to international threats, coordinate with the US State Department Diplomatic Security Service.
- Provide updated threat awareness and security briefings to court staff and presiding judges, and highlight incidents that could affect court operations.
- Conduct multijurisdictional training and exercises to reinforce communications, operational coordination, and other measures required to respond to threats or other incidents.
- Participate in information-sharing opportunities available through state or local fusion centers and the FBI's Joint Terrorism Task Force. Coordinate threat information and suspicious activity or behaviors with federal, state, and local judicial partners through a judicial protection working group.

Physical Security

- Determine how the trial and any proceedings will affect daily courthouse operations, including other cases.
- Establish secure ingress/egress routes to courthouses for prisoners and others associated with the trial; use of tent(s) or a temporary structure may provide cover for these routes.
- Arrange protective security details for judges, jurors, and witnesses, as necessary.
- Establish an annual or multiyear comprehensive, countywide security plan outlining the court's physical security profile and security protocols and procedures. Conduct pre-trial threat assessments to identify potential security risks. Adjust security posture based on physical or threat actor concerns.

^aCases that attract significant media or public attention and may include terrorism or high-profile drug trafficking cases or those that involve capital punishment or heinous crimes.

- Court staff should coordinate as early as possible with law enforcement agencies on security, judicial protection, response, and resource planning.
- Maintain procedures for screening and handling suspicious letters and packages. If encountered: do not disturb, handle, or open; evacuate the area; call 9-1-1; identify persons in the immediate discovery area for potential decontamination, medical treatment, or questioning.



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 on 11"x17" paper.

WARNING: Information contained in this document should not be taken as evidence of guilt or innocence and should not be relied upon for operational or enforcement action. Open-source reporting contained in this document is also not confirmation of its credibility or accuracy, nor does it imply NCTC's official view or endorsement.



Protecting High-Profile and High-Risk Court Proceedings Against Terrorist Threats *(continued)*

Suspicious Activity Reporting

Report suspicious activity before and during the trial to law enforcement or fusion centers. Categories of activity and behaviors that may be observed include:

- Misrepresentation: presenting false information or misusing insignia, credentials, documents, and/or identification in an attempt to access secure locations
- Expressed or implied threat: communicating a threat to cause death, bodily injury, or to damage or compromise the courthouse or surrounding facilities
- Theft/loss/diversion: stealing or diverting courthouse property (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents)
- Breach/attempted intrusion: unauthorized access or attempted access to secure or restricted courthouse areas
- Observation/surveillance: demonstrating unusual or prolonged interest in courthouse facilities, including filming, note-taking, or measuring distances, beyond mere casual or professional interest

Judges, Court Staff, Jurors, Witnesses and Other Personnel

- Provide uniformed or plainclothes law enforcement escorts for jurors or other personnel to/from the courtroom; secure judge's chambers and exterior perimeters such as parking areas
- Provide security awareness training for court staff and security personnel, covering essential security practices, court security plans, thresholds for reporting suspicious activities and threats, insider threat awareness, indicators of possible mobilization to violence, and behavioral threat detection training
- Train court staff and other officials as appropriate in countersurveillance, personal security techniques, and trauma medicine to identify and respond to potential threats. Consider incorporating the following: conducting perimeter and property sweeps; varying daily routines to avoid predictability; identifying different rally points for pick-up and drop-off.
- Limit the amount of information publicly available on social media, and refrain from posting professional

affiliations and personal details like home address, locational information, social events, and personal contacts

- Enhanced security for jury sequestration may include:
 - Working with law enforcement to vet on-site employees for potential connections to the suspect
 - Escorting sequestered jurors and visitors from hotel to court
 - Establishing on-site emergency evacuation procedures
 - Positioning security personnel in on-site locations such as recreation rooms, meal locations, and at the end of the hallways where jurors are staying
 - Limiting interactions with outside parties as permitted by law and in keeping with the First Amendment

Lawful Public Assemblies^b

- Individuals may lawfully assemble inside or outside the courtroom in connection with court proceedings. Terrorists may seek to use such gatherings as opportunities to incite violence or conduct attacks. Security should take such steps to protect all individuals without infringing on First Amendment-protected freedoms.
- Establish communication methods between court staff, law enforcement, fire, and emergency medical services to share information and coordinate planning and response efforts.

Public Information and Media

- Designate a single point of contact and location to provide official statements, answer media inquiries, serve as the liaison between the court, stakeholders, and the media, and help with logistics and technical requests.
- Review social media for activity that may raise public safety concerns for the court proceedings, including potential threats directed toward associated individuals or the court.
- Be familiar with state or local regulations that may prohibit the media from accessing the courtroom and proceedings.
- Anticipate large crowds and increased media interest that may require separate media facilities.

Cybersecurity

- Cases with increased attention may incite cyberattacks against court systems, databases, networks, or individuals involved in court proceedings. Assess information technology needs and incorporate potential security concerns into response and mitigation planning.
 - Beyond routine security precautions, additional restrictions on website traffic from potential malicious IP addresses may be required to prevent unauthorized access.
 - Implement network monitoring to identify activity that may fall outside of the typical range or standard.
 - Provide separate Wi-Fi access for users such as the media to reduce the network burden on the court's system and help identify and resolve issues should they arise.
- Provide recurring training to court staff about the range of cyber threats, best practices to safeguard sensitive data, and how court proceedings may impact threat vectors.
- Limit physical access to servers and network equipment.

Insider Threat

Witting or unwitting individuals who pose potential insider threats may exploit their access to critical systems, networks, facilities, or operations. Consider the following:

- Limit access credentials and routinely audit access-control records.
- Perform spot security checks of all interior and exterior areas.
- Ensure court staff are familiar with organizational policies and procedures to detect and deter insider threats through regular awareness training and an insider threat reporting mechanism.
- Throughout the proceedings, vary security screening and any inspections by including unpredictable and unannounced checks.

Resources

FBI Field Offices - <https://www.fbi.gov/contact-us/field-offices>

Joint Counterterrorism Assessment Team

First Responder's Toolboxes: Additional information about terrorist TTPs and response and mitigation considerations and can be found on JCAT's [website](#).

- [Awareness of Violent Extremist Tactics To Defeat Physical Security Can Improve Response](#)
- [Best Practices for Vehicle Screening Against Terrorist Tactics](#)
- [Complex Operating Environment—Attacks From Elevated Positions](#)
- [Complex Operating Environment—Special and Other Significant Events](#)
- [Postal and Shipping: Identification and Mitigation of Suspicious Mail and Packages](#)
- [Protection Considerations for Violent Extremist Threats to Public Officials](#)
- [Reporting Suspicious Activity—Critical for Terrorism Prevention](#)
- [Terrorist Insider Threat](#)
- [Vehicle-Borne Attacks: Tactics and Mitigation](#)

NCTC-DHS-FBI US VIOLENT EXTREMIST MOBILIZATION INDICATORS

<https://www.fbi.gov/file-repository/counterterrorism/us-violent-extremism-mobilization-indicators-2025-pdf/view>

^bThe Constitution guarantees the right to peaceable public assembly and free speech. 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.



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.