Operational Security Guide for Election Conferences

ELECTION SECURITY *Exchange*

Coalition of Election Association Leaders
A PROJECT OF ELECTION CENTER

Operational Security (OpSec) for election conferences is not about secrecy or limiting transparency. It is about protecting election officials, staff, vendors, and sensitive operational details from individuals who may exploit publicly available or casually disclosed information. Effective operational security strengthens safety, preserves operational integrity, and ensures election professionals can collaborate securely.

Use this guide as a companion to the **Operational Security Checklist for Election Conferences**, integrating best practices from election security guidance, OpSec training, and real-world conference security experience.

Before the Conference

Venue Selection

1 **Ensure meeting spaces can be isolated, access-controlled, and operationally secured.**

Venue selection should include evaluating whether: the facility provides 24/7 security presence; conference areas can be separated from public or lobby traffic; entire floors or dedicated spaces can be reserved; other groups will be present nearby; and whether the venue has prior experience hosting organizations with comparable security requirements. Thorough assessment of these factors helps reduce opportunities for surveillance, unauthorized access, disruptions, and infiltration while ensuring the environment can appropriately support the heightened operational security needs of election-related events.

2 **Require venues to prohibit public advertising or posting of conference-related information.**

Venues should restrict public disclosure of conference details, attendee information, and event-specific security-sensitive information. This limits opportunities for hostile actors, opportunistic disruptors, or unauthorized individuals to identify, monitor, or target the event, its participants, or associated operations.

Security Assessment and Law Enforcement Coordination

1. **Conduct a pre-event venue and internal security assessment prior to finalizing event plans.**

   Early assessments help identify physical, operational, and procedural vulnerabilities, allowing organizers to address risks related to unauthorized access, surveillance, social engineering, and facility weaknesses before the conference begins.

2. **Coordinate in advance with local/state law enforcement and/or fusion centers as appropriate.**

   Establishing relationships with external security partners before the event facilitates threat awareness, improves emergency preparedness, and ensures faster, more coordinated responses if security incidents or disruptions occur.

Incident Response Planning

1. **Plan for targeted disruptions and security incidents.**

   Election-related events may face threats such as swatting incidents, organized protests, credential abuse, harassment, suspicious packages, cyber intrusions, social engineering attempts, or unauthorized access. Advance planning for these scenarios strengthens preparedness, improves response coordination, protects personnel, and minimizes operational, physical, and reputational damage.

2. **Assign clear leadership roles, security responsibilities, and incident response chains.**

   Organizers should clearly define emergency response roles, crisis communications responsibilities, security decision-making authority, designated security leads, and formal incident reporting chains. Well-established authority and reporting structures reduce confusion, improve coordination, ensure timely decision-making, and strengthen overall response effectiveness during security incidents, disruptions, or emergencies.

3. **Evaluate and compare security staffing options to determine the most appropriate fit for the event.**

   Organizers should assess the strengths and limitations of off-duty law enforcement, private security providers, and venue-provided security personnel based on the event's threat environment, operational needs, authority to request identification from unknown individuals in secured areas, public visibility, response capabilities, venue familiarity, and budget. Careful evaluation helps establish the most effective security posture while balancing deterrence, emergency preparedness, and operational security.

4. **Identify secure rally points and emergency assembly locations.**

   Rally points should be carefully selected to minimize exposure to secondary threats, surveillance, congestion, confusion, or additional hazards during evacuations or disruptions. Poorly planned assembly areas can increase attendee vulnerability, while secure locations improve safety, accountability, and coordinated emergency response.

5 **Monitor public information channels to assess the evolving threat landscape before and during the conference.**

Monitoring social media and online discussions can provide early warning of threats such as planned protests, harassment campaigns, swatting threats, misinformation, doxxing, unauthorized attendee interest, or other emerging risks. Proactive awareness improves situational understanding, informs potential preventative steps, supports faster response, and helps organizers adapt security measures as conditions evolve.

6 **Conduct a final pre-conference physical and operational security walkthrough.**

A final walkthrough immediately prior to the event helps verify that security protocols, access controls, staffing, emergency procedures, and protective measures are fully implemented before attendees arrive, reducing overlooked vulnerabilities and minimizing last-minute security gaps.

Association/Conference Leadership Expectations

1 **Association/conference leadership should model strong operational security and adhere to standards consistently.**

Leadership behavior shapes organizational culture, reinforces security expectations, and significantly influences attendee, staff, and vendor compliance throughout the event.

2 **Reinforce personal safety and operational security messaging regularly before, during, and after the conference.**

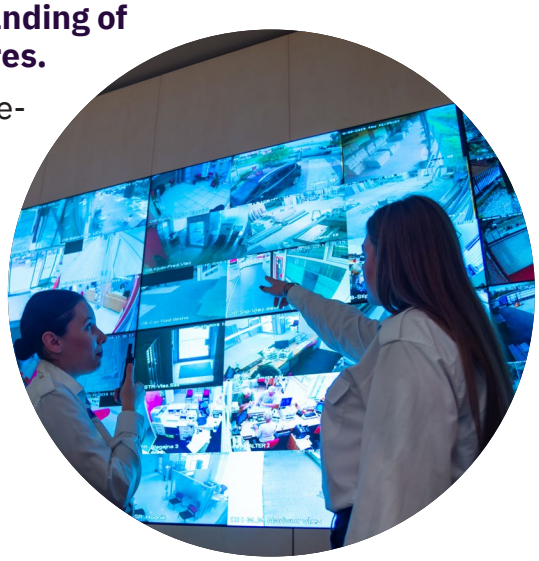
Repetition improves awareness, strengthens adherence, and helps maintain a proactive security mindset throughout the event lifecycle.

3 **Empower staff, vendors, and security personnel to enforce conference policies confidently and consistently without exception.**

Effective security requires organization-wide support, and empowered personnel improve enforcement reliability and reduce policy gaps.

4 **Ensure leadership maintains comprehensive understanding of conference security measures and response procedures.**

Leadership should understand both visible and behind-the-scenes security measures, operational vulnerabilities, and incident response protocols in order to guide attendees effectively, support security teams, make informed decisions, and maintain confidence during routine operations or crises.



Conference Preparation

1. **Require comprehensive registration, identity verification, and credentialing for all participants.**

   Attendees, vendors, speakers, staff, and other participants should be properly pre-registered, identity-verified, and credential-reviewed to prevent unauthorized attendance, reduce infiltration risks, and ensure appropriate vetting before access to sensitive election-related environments is granted.

2. **Use badges that minimize unnecessary identifying information.**

   Limiting visible personal or organizational details on badges reduces risks of doxxing, social engineering, credential targeting, and hostile actors gathering intelligence about attendees, staff, vendors, or their roles.

3. **Restrict access through centralized, controlled entry points.**

   Using primary controlled access points with credential checks and security screening improves monitoring, strengthens screening effectiveness, simplifies incident response, and reduces opportunities for unauthorized entry.

4. **Train frontline personnel for security awareness and response.**

   Registration staff, security personnel, and other frontline event staff serve as the earliest line of defense and should be equipped to recognize suspicious behavior, credential anomalies, unauthorized access, and social engineering attempts, and to apply appropriate de-escalation techniques. Effective training improves prevention, strengthens access control enforcement, enhances response capabilities, reduces unnecessary confrontation, helps prevent tailgating or policy circumvention, and reinforces a strong security culture throughout the event.

Communication/Media Guidelines

1. **Protect sensitive conference information through comprehensive communications security policies.**

   Conference organizers should restrict public posting or distribution of locations, detailed agendas, room assignments, attendee lists, speaker details, and other security-sensitive operational information while establishing clear media, photography, social media, and public communications policies for attendees, staff, vendors, and press. Effective controls define authorized communications channels and restrict unauthorized photography, recording, livestreaming, or public disclosures that could expose sensitive operational details.

2 **Limit publicly shared agenda details and distribute sensitive conference scheduling information through secure attendee channels.**

Public-facing agendas should minimize operational exposure by limiting public-facing details to session titles only, where appropriate. Limit the public exposure of speaker names, attendee-specific information, or sensitive session logistics in publicly available documents. Detailed schedules, speaker information, and session-specific operational details should be shared privately through secure attendee channels to protect operational timelines, reduce adversarial intelligence gathering, and minimize opportunities for surveillance, targeting, or exploitation of vulnerable conference moments.

3 **Review all presentation materials, handouts, signage, and digital displays for sensitive operational, security, or personal information before release.**

Pre-screening materials helps prevent inadvertent disclosure of facility details, election procedures, staff information, system vulnerabilities, or other intelligence that could be exploited by malicious actors.

4 **Establish, distribute, and enforce comprehensive participant conduct policies before and during the event.**

Participants should receive clear pre-conference guidance outlining behavioral expectations, Code of Conduct standards, security requirements, operational responsibilities, personal safety practices, enforcement consequences, and applicable disciplinary actions. Early and transparent communication strengthens security awareness, reinforces protective behaviors, reduces misunderstandings, and ensures all participants understand their role in reducing operational, physical, and digital security risks. Consistent enforcement preserves credibility, strengthens deterrence, and reinforces commitment to the conference's overall security posture.

Attendee Conference Preparation

1 **Require attendees to review, acknowledge, and commit to all conference security, operational security, conduct, and safety requirements prior to participation.**

Attendees should understand and formally acknowledge applicable security guidelines, behavioral expectations, operational restrictions, and personal safety requirements before travel or event participation. Early review and commitment strengthen compliance, reinforce accountability, reduce misunderstandings, and help ensure all participants actively support the conference's overall security posture.

2 **Prohibit attendee social media posting and public sharing of conference-related activities during travel and throughout the event.**

Individual participant behavior remains a critical operational security factor. Restricting attendee posting helps prevent inadvertent disclosure of travel patterns, schedules, attendee identities, operational timelines, or sensitive conference activities that hostile actors could exploit.

3 **Reduce unnecessary digital exposure on attendee devices prior to travel.**

Disabling location services, Bluetooth auto-connect, and other non-essential wireless features helps minimize metadata leakage, tracking risks, wireless exploitation, and opportunities for adversaries to gather movement or operational intelligence.

During the Conference

Conference Leadership/Staff

1 **Secure and clearly designate restricted or sensitive operational areas.**

Staff-only, restricted, and sensitive areas should be identified and reinforced through signage, physical barriers, and controlled access measures to reduce accidental or intentional unauthorized entry while protecting sensitive operations, personnel, and information.

2 **Maintain continuous physical security oversight across all conference spaces.**

Hallways, entrances, meeting rooms, vendor spaces, common areas, and restricted zones should be continuously monitored through active oversight and periodic security sweeps. These help detect suspicious activity, hostile surveillance, unauthorized access, suspicious or unattended bags or packages, or evolving security concerns before they escalate into larger incidents.

3 **Enforce badge, credential, and access control requirements consistently throughout secured conference spaces.**

Uniform enforcement of badge display, credential verification, and access policies preserves the integrity of the security plan, prevents unauthorized access, and reduces opportunities for social engineering, credential abuse, or policy circumvention. Even when most organizers and attendees know each other, consistent enforcement remains critical to reducing risk.

All Conference Attendees

1 **Limit visible conference identification outside secured event spaces.**

Attendees should avoid wearing badges, branded apparel, or other visibly identifiable materials in public settings to reduce risks of surveillance, harassment, targeting, social engineering, or hostile actors linking individuals to election-related activities.

2 **Protect sensitive materials, devices, and operational information from unauthorized exposure or access.**

Sensitive documents, laptops, mobile devices, presentation screens, and printed materials should be secured through privacy screens, strong device security settings, physical safeguards, and proper storage when unattended. Comprehensive physical and digital protections reduce risks of shoulder surfing, unauthorized photography, theft, data compromise, information leakage, and inadvertent disclosure of operational or security-sensitive information.

3 **Use only trusted, secure communication networks for conference-related activities.**

Public Wi-Fi networks increase exposure to cyber intrusions, interception, credential theft, and other malicious activities. VPNs, secure hotspots, and other protected communication methods strengthen data protection, reduce interception risks, and better safeguard sensitive operational and election-related information during travel and throughout the conference.

4 **Limit the use of unsecured personal devices for sensitive conference or operational activities.**

Personal devices often present increased cybersecurity vulnerabilities, inconsistent security controls, and expanded attack surfaces. Sensitive conference, operational, or election-related business should only occur on properly secured devices to reduce risks of compromise or unauthorized disclosure.

5 **Strengthen attendee awareness of social engineering, public-space vulnerabilities, and human intelligence threats.**

Attendees, staff, and vendors should understand that conference venues, hotels, restaurants, transportation hubs, and other public or semi-public spaces may serve as intelligence-gathering environments where casual conversations, visible materials, or operational discussions can unintentionally expose sensitive information. Training should also address phishing, impersonation, credential harvesting, and broader social engineering attempts. Strong awareness reduces risks of eavesdropping, surveillance, unauthorized disclosures, credential compromise, and broader security breaches. Consider a brief session at the beginning of the event to communicate these critical protective measures to all participants.

3. After the Conference

All Conference Attendees

1 **Remove or conceal visible conference identification during departure and post-event travel.**

Attendees, staff, and vendors should remove or conceal badges, credentials, and identifiable conference materials before leaving event spaces to reduce ongoing risks of surveillance, harassment, targeting, or adversarial identification after the conference concludes.

2 **Maintain operational discretion during post-event travel and public settings.**

Attendees, staff, and vendors should avoid discussing sensitive conference activities, attendee details, security procedures, or operational matters while traveling home or in public post-event environments, as threat actors may continue monitoring participants and post-conference disclosures can create delayed security vulnerabilities.

3 **Securely transport, handle, and store sensitive materials following event conclusion.**

Conference materials, devices, and sensitive documents should remain properly secured during departure and return travel to prevent loss, theft, unauthorized disclosure, or compromise of operationally sensitive information.

Conference Leadership/Staff

1 **Implement secure post-event data retention, disposal, and archival procedures.**

Organizers should remove, destroy, or securely dispose of unnecessary temporary records, access lists, printed materials, and nonessential sensitive data. Essential records, security documentation, incident reports, and operational materials should be securely archived. Strong data hygiene reduces long-term exposure, lowers breach risks, preserves institutional continuity, and ensures critical information remains protected yet accessible for future planning or security needs.

2 **Conduct a comprehensive post-event security review, communications assessment, and continuous improvement process.**

Organizers, security personnel, and relevant partners should formally evaluate conference security performance, document incidents, suspicious activities, and policy violations, and assess participant compliance with operational and other security protocols. Organizers should be prepared to review public communications, social media content, event materials, and post-event messaging for inadvertent disclosures or operational security failures, and to update security, communications, and incident response procedures based on lessons learned. Comprehensive review strengthens institutional knowledge, improves preparedness, identifies vulnerabilities,and ensures future conference security remains responsive to evolving threats.