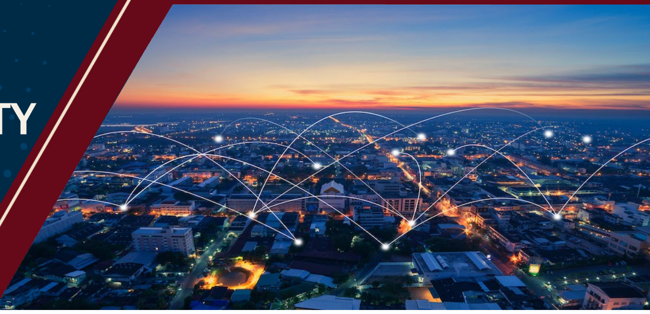

GUIDE TO OPERATIONAL SECURITY FOR ELECTION OFFICIALS

Overview

Operational security (OPSEC) is a systematic process for identifying and protecting sensitive information, data, or capabilities within an organization.[1] OPSEC is not out of reach for any office. It is something people do every day in their personal and professional lives when they take actions to protect information that they know could create risk if exposed—like safeguarding your social security number and date of birth to protect against identity theft. OPSEC is also a critical part of protecting election infrastructure. Without adequate safeguards in place, sensitive information can be exposed, whether wittingly or unwittingly, and collected by potential threat actors, like foreign adversaries and criminals. This may impact the ability of election workers to perform their official duties, expose voters' personally identifiable information (PII), or enable unauthorized access to internal systems or facilities. By embedding OPSEC principles in day-to-day election operations and fostering a shared culture of security throughout their organization, election workers can reduce the likelihood of disclosing sensitive information to unauthorized parties. Good OPSEC can be achieved while also maintaining a transparent election process and responding to public inquiries.

Example: Voters' Sensitive Information Shared

A local election jurisdiction accidentally shared a spreadsheet in response to a public records request that included the last four digits of voters' social security numbers. When the error was discovered, the jurisdiction asked the requestor to delete the sensitive information and was able to confirm they did so. The jurisdiction later sent letters to approximately 500,000 affected registered voters to notify them of the incident and corrective action.

Example: Voting System Manufacturers' Webstores and Jurisdiction Training Manuals Displayed Images of Physical Equipment Keys

Using publicly available information, potential adversaries could have reproduced or procured physical keys to locks used to protect voting equipment. At times, online imagery featured physical key information, such as key cuts or key-codes, which could be used to identify the types of keys needed to access internal pieces of equipment.

Transparency and information sharing are vital components of election administration, and the recommendations included in this guide are consistent with these aims. OPSEC helps organizations consider data and information from an adversary's point of view, enabling a holistic assessment of sensitive data and potential malicious or unauthorized use cases. Even if individual pieces of information do not seem particularly sensitive in nature, multiple pieces of information about an organization, its operations, or its people can potentially be pieced together to create far greater risk. With training and awareness of OPSEC principles, election workers can better understand these aggregated risks and limit the potential exposure of sensitive information.

This resource provides an overview of OPSEC in an election context, highlighting potential risks and real-world examples, and offers election infrastructure owners and operators mitigation activities to consider.

[1] National Institute of Standards and Technology, Computer Security Resource Center (CSRC) Glossary: Operational Security (OPSEC). https://csrc.nist.gov/glossary/term/operations_security#:~:text=Definitions%3A%20Systematic%20and%20proven%20process%20by%20which%20potential,of%20the%20planning%20and%20execution%20of%20sensitive%20activities.

Implementing OPSEC Principles

The following five steps help election workers improve processes and procedures to better protect sensitive information by implementing OPSEC principles. For a more detailed worksheet, please refer to Appendix A.

- **Step 1 – Identify Sensitive Information:** Develop an organizational understanding of all data, assets, and personal information that would provide valuable information to an adversary, whether on its own or in aggregation.
- **Step 2 – Understand Threats:** Understand the tactics used by threat actors that can present physical, cyber, or operational risks.
- **Step 3 – Identify Vulnerabilities:** Identify potential vulnerabilities in physical and cybersecurity procedures that could allow an adversary access to sensitive information identified in Step 1.
- **Step 4 – Assess Risks:** Considering the threats identified in Step 2 and the vulnerabilities identified in Step 3, assess the likelihood and severity of a threat actor's actions on the security of election infrastructure or processes if they had access to sensitive information from Step 1.
- **Step 5 – Implement Countermeasures:** Select and implement countermeasures that eliminate or reduce the priority risks identified in Step 4.[2]

Adversary Methods of Collection

When implementing OPSEC principles, it is important to think through how adversaries can aggregate sensitive pieces of information, referred to as *indicators,* to form a bigger picture of organizational vulnerabilities. Indicators may be collected through a variety of activities, including:

- Viewing social media pages
- Going through recycling or trash
- Aggregating information from multiple sources like emails, websites, or contract proposals
- Observing election offices and staff or eavesdropping on conversations
- Reviewing public records for mistakenly disclosed security information
- Social engineering

[2] National Institute of Standards and Technology, Computer Security Resource Center (CSRC) Glossary: Operational Security (OPSEC). https://csrc.nist.gov/glossary/term/operations_security#:~:text=Definitions%3A%20Systematic%20and%20proven%20process%20by%20which%20potential,of%20the%20planning%20and%20execution%20of%20sensitive%20activities.-

Application of OPSEC Countermeasures

OPSEC countermeasures reduce the likelihood that critical information will be unintentionally disclosed to threat actors and should be applied to all election security risk areas, including people, operations, cybersecurity, and physical security. The following table includes examples of applying OPSEC countermeasures across different risk areas.

Risk Areas	Applying OPSEC Countermeasures
People	▪ Where possible, avoid posting details about work-related activities, travel plans, schedules, or locations publicly. ▪ Disable location services on apps and devices where you do not need those functions to reduce the risk of adversaries obtaining metadata that could inform of sensitive locations. ▪ Do not share photos that make a location obvious in real time. ▪ Avoid discussing sensitive information in public, or near spaces with public access, which may be overheard by unauthorized individuals. ▪ Avoid publicly displaying unique personal details that can be aggregated to reveal identity and location, such as bumper stickers. ▪ Consider making personal social media accounts private. ▪ Consider regularly requesting that personal information be removed from public records websites. ▪ Enable multi-factor authentication on your accounts and use complex password phrases.
Operations	▪ Conduct regular awareness training with all staff on protecting sensitive information and understanding opportunities for exploitation. ▪ Create or update organizational guidelines for protecting sensitive data to prevent it from being accidentally released or leaked. ▪ Create or update organizational guidelines for disposing physical and digital information securely. ▪ Apply sensitivity markings to all documents to indicate the type of information and level of distribution, as applicable.
Cybersecurity	▪ Secure infrastructure details, such as information about specific commercial services, network diagrams, and security information. ▪ Thoroughly review and redact sensitive information to avoid accidental disclosure through public records requests, in accordance with applicable state laws. ▪ Avoid use of personal devices for official business, which opens additional vectors for compromise.
Physical Security	▪ Discourage staff from wearing badges or other forms of identification publicly outside of work. ▪ Restrict access to facility floor plans, especially plans that reveal security access points and where sensitive equipment is stored in an election facility. ▪ Regularly review materials such as manuals, training videos, and educational content, for inadvertent disclosure of sensitive physical security information.

Conclusion

Just as elections are continuous operations, the cycle for reviewing and updating OPSEC practices should be applied continuously across every aspect of an organization to prevent the disclosure of sensitive information. Through careful planning, documentation, and training, applying OPSEC principles can help election officials further safeguard election infrastructure from potential threat actors. OPSEC principles should also evolve to meet a changing threat environment and new threat actor tactics.

Further Resources Related to OPSEC

The information provided in this document is complemented by additional resources on OPSEC from CISA and CISA's federal partners linked below. Election stakeholders are encouraged to review these resources to further prepare for and mitigate risks associated with potential OPSEC incidents.

- CISA Election Infrastructure Insider Threat Mitigation Guide: https://www.cisa.gov/resources-tools/resources/election-infrastructure-insider-threat-mitigation-guide
- CISA Physical Security of Voting Locations and Election Facilities: https://www.cisa.gov/resources-tools/resources/physical-security-voting-locations-and-election-facilities
- CISA Personal Security Considerations Action Guide: https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide
- U.S. Election Assistance Commission (EAC) Best Practices: Public Records Request: https://www.eac.gov/election-officials/best-practices-public-records-request
- National Counterintelligence and Security Center OPSEC Posters and Templates: https://www.dni.gov/index.php/ncsc-what-we-do/operations-security
- National Institute of Standards and Technology (NIST) Definition of Operational Security: https://csrc.nist.gov/glossary/term/operations_security

APPENDIX A: STEPS TO IMPROVE OPERATIONAL SECURITY

OPSEC Step	Best Practice/Implementation Details
Step 1 – Identify Sensitive Information: Develop an organizational understanding of all data, assets, and personal information that would provide valuable information to an adversary, whether on their own or in aggregation.	**Identify and conduct routine reviews of all sensitive information.** • Form a multi-disciplinary team to identify sensitive information. • Develop a list that provides an inventory of sensitive information. • Confirm records or documents that need to be evaluated for inclusion in the sensitive information list. • If a new service or new service provider is used, review their information for any potential inclusion on the sensitive information list. • Train team members, including key stakeholders and your legal team (within and outside your office), on the sensitive information list. • Establish a routing process so the multi-disciplinary team can review information or data request material prior to sharing with the requestor, such as with public records requests.
Step 2 – Understand Threats: Understand the tactics used by threat actors that can present physical, cyber, or operational risks to election infrastructure or processes.	**Assess potential threats and review this assessment periodically.** • Identify who is the threat actor (foreign adversaries, criminal actors, etc.) and what is their objective. • Consider what systems or information a threat actor may target based on their objective. • Understand the threat actor's capabilities and sophistication level. Can they do it themselves or will they require assistance, such as potential insider assistance?
Step 3 – Identify Vulnerabilities: Identify potential vulnerabilities in physical, cyber, and operational procedures that could allow an adversary access to critical information.	**Assess threats that may exist to the sensitive information identified in Step 1.** • Identify potential risk and vulnerabilities in election infrastructure and processes that may lead to exposure of sensitive information identified in Step 1, based on adversarial capabilities identified in Step 2. • When reviewing potential risk, consider an all-hazards approach (e.g., physical, cyber, information attacks).
Step 4 – Assess Risks: Consider the likelihood and severity of a threat actor's actions on the security of election infrastructure or processes if they had access to sensitive information.	**Assess the risks presented by the vulnerabilities documented in Step 3.** • Review the likelihood or probability of the threat occurring, and then the severity of the impact (low, significant, catastrophic, etc.) if that threat did occur. • Consider vulnerabilities/impact/probability from the perspective of the information security triad of Confidentiality, Integrity, and Availability. • Prioritize the risks and implement a plan of action.
Step 5 – Implement Countermeasures: Select and implement countermeasures that eliminate or reduce risk.	**Configure policies/processes/controls/devices that can be implemented to mitigate the risks from Step 4.** • If you cannot action everything, start with the priority risks. • Create processes to verify entities asking to receive information; implement two-party control/monitoring of critical operations and assets; utilize physical and electronic ID verification methods. • Develop notification procedures for reporting potential OPSEC violations, and steps to respond and recover if a potential violation becomes an incident. • Conduct regular training exercises to test mitigation plans for responding to unauthorized disclosure of sensitive information. • Develop and be prepared to use holding statements and other pre-prepared communications materials when an incident occurs.

	• Review stakeholder contact lists for accuracy. • Review identification verification procedures to ensure mitigation plans are resistant to social engineering (i.e., does everyone know current “challenge or pass phrases” and when they rotate?). • Use scenarios to test your plan’s ability to respond appropriately to mitigate the fallout from a disclosure. For example: ○ A list of voting system administrative usernames and passwords is stolen. ○ PII from a voter registration list is erroneously sent to an unauthorized party. ○ A list of confidential voters is erroneously sent to a media organization. ○ Vulnerability scanning reports from a recent cybersecurity scan or results of a recent penetration test are discovered to have been emailed to an untrusted party.