INSIDER THREAT MITIGATION FOR ELECTION INFRASTRUCTURE
Insider Threats to Critical Infrastructure

- Organizations of all types and sizes are vulnerable to insider threats
- Organizations may experience losses including:
  - Physical damage to critical infrastructure
  - Disruption of productivity
  - Intellectual property theft
  - Accidental leakage of sensitive data
  - Damage to an organization’s reputation
Many individuals are involved in administering an election, providing an opportunity for bad actors.

Privileged digital and/or physical access creates the possibility of exploitation or compromise.

Practices that deter, detect, or prevent harm caused by insiders are integral to conducting secure elections.
Defining Insider Threats

**Insider Threat:** the potential for an insider to use their authorized access or special understanding of an organization to harm that organization.

*Types of Harm:*
- Malicious
- Complacent
- Unintentional

*Areas of Impact:*
- Organization
- Data
- Personnel
Unintentional Threats

Examples of Unintentional Threats

- Entry “piggybacking”
- Misplacing or losing a device
- Ignoring security updates or patches
- Mistyping an email address
- Clicking on a phishing email
- Improperly disposing of sensitive documents

Accidents

- Mistakes can happen
- Risk can be reduced through training and control measures

Negligence

- Result of carelessness
- Behaviors can be witnessed and corrected
Intentional Threats

Examples of Intentional Threats

- Inappropriately altering or destroying data
- Intimidating or threatening staff
- Allowing unauthorized access
- Leaking confidential information
- Stealing equipment
- Turning off security cameras

Collusion

- Collaboration with an external threat actor
- Threat actors typically well-versed in avoiding detection

Third-Party Threats

- Contractors or vendors who have been granted temporary access
Expressions of Insider Threat

- Cybersecurity Incidents
- Violence
- Espionage
- Sabotage
- Theft
Information Environment

The spread of election-related mis-, dis-, and malinformation (MDM) may provide an additional motivation for insider threats.

MDM narratives can be especially attractive to individuals already experiencing other stressors in their life.

These narratives often provide an interpretation of reality that is more coherent to the affected individual than real life.

**Common Tactics of MDM Actors:**
- Create a sense of belonging among followers
- Build community
- Foster an in-group or “us vs. them” mentality
Building an Insider Threat Mitigation Program

Establishes a standard baseline for election roles and responsibilities

Provides an auditable record of asset transfers and transactions

Grants only the physical and digital access necessary for job functions

Explicitly verifies every request for access to systems or data
Election Insider Threats in Focus

Consider these best practices when procuring services from third-party vendors, contractors, temporary staff, seasonal staff, and volunteers.

- **Code of Conduct**
- **Same high security standard**
- **Strong recruitment & procurement**
- **Mandatory background checks**
- **SOPs and regular retraining**
- **Identifying items (lanyard badge, vest)**
- **Two-person rule**
- **Restrict or eliminate remote access**
Building Resilience to MDM

While it is impossible to predict or fully control the information environment around elections, election infrastructure stakeholders can educate and build resilience with their staff, volunteers, and vendors and reduce susceptibility to MDM threats.

- Cultivate a **shared sense of community and mission** among all members of the organization
- Communicate **proactively, consistently, and transparently** about your work (both internally and externally)
- Conduct ongoing **training and education** with all team members to raise awareness of MDM narratives and tactics
Building a Culture of Reporting

- A positive, open organizational culture includes:
  - Encouraging ongoing learning and asking questions
  - Transparent mechanisms for reporting and accountability when reporting occurs

- Distinguishing whistleblowing from insider threat
  - Whistleblower knows appropriate procedures and reporting pathways
  - Not exploiting or intending harm
  - Protected act for federal employees

“Whistleblowers perform an important service by reporting what they reasonably believe to be evidence of waste, fraud, abuse, or mismanagement.” – Department of Homeland Security
Conclusion

1. Foster a **positive, supportive** culture
2. Be **transparent and consistent**
3. Emphasize **shared mission**
4. Report and intervene **early**
5. Conduct a **debrief**
Ryan Macias
Election Security SME Consultant

electionsecurity@cisa.dhs.gov

Contact CISA:
Central@cisa.dhs.gov