Defending Digital Democracy Project

1. **Convening leaders** from tech sector, government, academia, and the media to develop best practices for basic risk mitigation steps and implementation.

2. **Helping those on the frontline**—campaigns and election officials—understand the risks they face from cybersecurity and information operations.

3. **Providing practical “playbooks”** to improve readiness.

4. **Emphasizing training and preparedness** as fundamental to success—a plan is only as good as its execution.

5. **Empowering policymakers** to better understand the issues so they can become more effective advocates.
State and Local Election Cybersecurity Playbook
Protect the integrity of the elections process and preserve the public’s confidence in the system.
S&L Playbook Components

- **Playbook Approach**
- **Common Ground**
  - 10 Best Practices for All Election Jurisdictions
  - Research Insights by Election System
- **Technical Recommendations by System**
  - Voter Registration Databases
  - Vote Casting Devices
  - Vote Tallying Systems
  - Election Night Reporting
  - Internal and Public-Facing Communications
- **Appendices**
  - Vendor Selection and Maintenance
  - Election Audits
  - External Resources
Potential Malicious Actors

**POSSIBLE ACTORS**
- Nation-State Actors
- Black Hat Hackers
- Terrorists
- Insiders
- Politically Motivated Groups

**POSSIBLE MOTIVATIONS**
- Financial Gain
- Retribution for Perceived Grievances
- Fame and Reputation
- Sow Social Division
- Foment Chaos / Anarchy
- Subvert Political Opposition
- Foreign Policy / National Interests
- Undermine Trust in Democracy
Common Tactics: Cyber Operations

- Hacking
  - SQL Injection
  - Port Scans
  - Man-in-the-Middle

- Social Engineering
  - Spear-Phishing

- DDoS (Distributed Denial of Service)
- Insider Threat
Information Operations (IO) includes propaganda, disinformation, and other tools used to manipulate public perception.

- Leaking Stolen Information
- Spreading False Information
- Amplifying Divisive Content
- Manipulating Public Facing Communications
Elections as a System of Systems

Election System Overview: Potential Attack Vectors

1. Voter Registration Database System
2. e-Pollbooks / Onsite Voter Registration System
3. Vote Capture Devices
4. Vote Tally System
5. Election Night Reporting System

Traditional and Social Media (National and Local)
Election Officials’ Communications
State and Other County Systems
Vendors
10 Best Practices for All Jurisdictions

1. Create a proactive security culture.
2. Treat elections as an interconnected system.
3. Have a paper vote record.
4. Use audits to show transparency and maintain trust in the elections process.
5. Implement strong passwords with two-factor authentication, and change defaults.
10 Best Practices for All Jurisdictions

6. Control and actively manage access.

7. Prioritize and isolate sensitive data and systems.

8. Monitor, log, and backup data.

9. Require vendors to make security a priority.

10. Build public trust and prepare for information operations.
Where State Legislatures Can Make the Most Impact

- Implement 2FA
- Isolate sensitive data systems
- Implement audit logs and monitoring
- Have a paper trail
- Do vote audits
- TRAIN
National Conference March 26 & 27 2018

TTX Train the Trainer Event

Day 1: Threat Briefs, TTX, and AAR

Day 2: How to Build and Execute a TTX

38 States & 120 Election Officials
Defending Digital Democracy Project

FOLLOW US @D3P
FOLLOW US /DEFENDINGDIGITAL
SHARE WITH #SECUREELECTIONS