ELECTION INFRASTRUCTURE RISK

PROCESS

1. REGISTRATION

- Voter Registration

2. POLLBOOK

- Pollbook Preparation
- Pollbook Use

3. VOTING MACHINE

- Ballot Preparation
- Voting Machine Preparation
- Voting Machine Use

4. TABULATION

- Tabulation Use (Precinct)
- Tabulation Use (Central)
- Aggregation (State)

5. WEBSITE

- Website

RISK ASSESSMENT

INTEGRITY ATTACKS

Integrity attacks on state-level voter registration systems, the preparation of election data, vote aggregation systems, and election websites present particular risk to the ability of jurisdictions to conduct elections.

AVAILABILITY ATTACKS

Availability attacks on state or local-level systems that support same-day registration, vote center check-in, or provisional voting also have the potential to pose meaningful risk to the ability of jurisdictions to conduct elections.

VOTING SYSTEMS

Voting systems present a high consequence target for threat actors but low likelihood of successful attacks at scale, meaning that there is lower risk of incidents when compared to other infrastructure components of the election process.

DIVERSE INFRASTRUCTURE

U.S. election systems are comprised of diverse infrastructure and security controls. However, even jurisdictions that implement cybersecurity best practices are potentially vulnerable to cyber attack by sophisticated cyber actors.

DISINFORMATION CAMPAIGNS

Disinformation campaigns related to election infrastructure can amplify disruptions of electoral processes and erode public trust in election results.