Appendix C

Threat	Vulnerability	Likelihood	Impact	Risk	Mitigation Measures
Cyber threats					
Phishing attacks	Election officials and voters susceptible to phishing emails	High	Election data compromise, voter suppression	High	Public awareness campaigns, multi-factor authentication (MFA), email filtering.
Denial-of-Service (DoS) attacks	Online voting servers vulnerable to excessive traffic	High	Disruption of online voting, system downtime	High	Implement traffic filtering, cloud-based DoS mitigation services, redundancy in infrastructure
Insider threats	Election staff with excessive privileges	Medium	Tampering with election results	Medium	Strict access controls, continuous monitoring, background checks
Supply chain attacks	Compromised voting software and hardware providers	Medium	Election manipulation	Medium	Vendor risk assessment, third-party audits, software code review, digital signatures
Operational Threats					
Voter registration database breach	Weak authentication and encryption mechanisms	Low	Unauthorized data access, voter fraud	Low	Encryption, strict access controls, intrusion detection systems
System downtime	Lack of redundancy and failover mechanisms	Low	Voter disenfranchisement	Low	Load balancing, backup systems, regular testing
Physical Threats					
Tampering with voting devices	Lack of physical security measures	Low	Alteration of election outcomes	Low	Tamper-proof hardware, routine audits, chain of custody procedures
Power outages	Lack of backup power sources	Medium	Voting system failure	Medium	Uninterruptible power supply (UPS), backup power sources
Social engineeri	Election officials	Medium	Unauthorized access to election data	Medium	Regular security training, strict

	susceptible to deception				verification protocols