MEET the THREAT

States Confront the Cyber Challenge

Securing Election Infrastructure

The Threat to Voting Systems

The people of the United States are committed to free and fair elections. With the 2016 elections fast approaching, state and local officials are focused on fulfilling their legal responsibility to safeguard the key components of the voting process: voter registration databases, voting records, and election management systems. Experts acknowledge that a malicious actor could exploit software vulnerabilities on or before election day to undermine the integrity of voter data or the availability of voting systems, and hackers recently targeted voter registration databases in at least two states. Although the compromise of such data is unlikely to undermine the validity of election results, targeted attacks could fuel accusations of impropriety. Fortunately, states and localities can enforce present procedures and institute short-term precautions to counter perceptions that computer-assisted voting threatens the democratic process.

Questions for Governors

- Who is responsible for regulating federal, state, and local elections in my state?
- What kind of computer-assisted voting is available, and in what voting districts?
- What are the possible avenues by which attackers could disrupt or manipulate voting via computer?
- How are officials testing and certifying computer-assisted voting systems?
- What contingency plans exist should computer-assisted voting systems go down?
- What have state and local officials done to secure voter registration databases, and what more could they do?
- How will officials ensure they can detect any vote manipulation that does occur?
- Who is responsible for responding to a security breach of voting systems and mitigating the consequences?

Recommended Steps for Governors

(1) *Receive a briefing from your Secretary of State or other relevant officials on the present status and testing of all computer-assisted voting systems, including overseas ballot returns, and conduct a risk assessment*.

With only months to go before the 2016 elections, and equipped with limited resources, states should use a risk-based approach that focuses on the most serious cyber threats to voting systems. The first step is a risk assessment that takes stock of voting systems, identifies the potential threats to each one, and prioritizes any vulnerabilities.

(2) *Ensure that all polling stations produce and preserve as many paper records as possible*.

Hard copy records are invulnerable to cyber attacks. Many voting machines acknowledge this by printing so-called Voter Verified Audit Paper Trails (VVAPTs), which are essentially paper receipts that allow a voter to confirm their vote before the voting machine writes their anonymous ballot selection into computer memory. While VVAPTs do not prevent cyber attacks against the voting machines that produce them, they provide a mechanism for detecting an attack after the fact, and preserve a record of the voter's true selection. However, many voting districts use voting machines that do not produce VVAPTs. Governors should work with state and local officials to offset this weakness by generating other paper records in accordance with the law. For example, paper entry logs at polling places can be used to verify results by checking voter participation against the vote totals.

(3) *Ensure that districts back up voter rolls and poll books*.

Criminals have targeted voter data held by states. Such intrusions could allow malicious actors to restrict the franchise by denying eligible voters access to polling stations in states that do not allow same-day voter registration. Backing up registration data and electronic poll books—including with paper copies or compact discs—is a simple and effective way to meet this particular threat.

(4) *Train election officials and poll workers to follow existing procedures and institute common-sense security measures*.

Many of the procedures already in place to help guarantee free and fair elections also guard against cyber attacks and their effects. Ensuring that election workers follow such existing rules will go a long way toward blocking any criminal efforts to disrupt or manipulate voting on election day. Additionally, governors can work with voting districts to instill reasonable computer security precautions that some officials might currently overlook. For example, poll workers should not use any computers with out-of-date software that is likely to have security vulnerabilities.

(5) *Identify and inventory the make, model, certification status, and vulnerability mitigation strategy for every type of voting system*.

Federal, state, and local officials have already decertified various voting systems that are vulnerable to cyber attacks. Governors of states that continue to use such systems should ask relevant jurisdictions to describe their strategies for mitigating any vulnerabilities. Officials should consider decertifying vulnerable machines in those jurisdictions without any mitigation plans. Documenting the review process will support legal and policy arguments for decertification decisions.

(6) *Engage all stakeholders to develop an ad-hoc framework that allows for independent experts to react quickly and triage security issues that emerge before, during, or after the election*.

In the event that a cyber incident does affect voter registration information, voting systems, or election management systems, Governors should already have an established governance framework for the response. Such a framework would enable quick coordination and communication between the governor's office, independent experts, local election officials, political parties, and political campaigns. Of course, any such arrangement would need to account for federal, state, and local laws regulating communication between campaigns and election officials.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*