NASS
National Association
of Secretaries of State

April 2020

ISSUE BRIEFING: State Spending of Election Security Grant Funds

Congress allocated $380 million to states through the Help America Vote Act (HAVA) in March of 2018 and required states to provide a five percent match. These 2018 HAVA funds were for efforts to improve the administration of elections for federal office, including to enhance election security and make election security improvements. In December of 2019, Congress provided an additional $425 million for these same purposes and required a 20 percent match from states.

In March of 2020, Congress allocated $400 million dollars in additional HAVA funds within the Coronavirus Aid, Relief, and Economic Security (CARES) Act for state efforts to prepare for and respond to the impact of the COVID-19 pandemic on elections. Prior to the release of the CARES Act funding, the U.S. Election Assistance Commission (EAC) issued special guidance allowing states to use their HAVA funding to address the impact of the pandemic on elections, including personal protective equipment (PPE) for staff and poll workers, increased use of absentee and vote-by-mail, and sanitizing voting equipment and polling locations.

Consistent with the purpose of the 2018 and 2019 HAVA funding, states have developed multi-year plans to spend the money towards improving the security of their election infrastructure. The specific use and timeframe for spending varies based on factors unique to each state, including the age/functionality of existing technology, cybersecurity risks, the type of voting equipment used, voting methods and procedures, and the role of state versus local officials in election administration. In addition, states may face issues in accessing and utilizing the funds, including legislative approval requirements, procurement regulations, and budget constraints impacting the required state match. Also, reports of state expenditures may not reflect funds that have been obligated (but not yet spent) for products or services. Some states distribute funds over several years to support long-term programs and personnel.

While the specific use of the election security funds varies among states, there are some general trends in how states have been are using the money, including[1]:

- Security upgrades and enhancements to election management systems, voter registration databases, election night reporting, and other election related IT infrastructure
- Purchase of new voting equipment, e-poll books, computer systems, etc.
- Hiring of election security personnel
- Implementing multi-factor authentication
- Developing post-election audit procedures
- Establishing Cybersecurity Navigator programs
- Conducting cybersecurity risk and vulnerability assessments and implementing mitigation efforts
- Developing incident preparedness/management plans and exercises
- Developing election security communication/notification plans
- Providing cybersecurity training for state and local election officials
- Providing election security grants to counties/local jurisdictions

[1] Information on state spending of election security grants funds is based on budget narratives and financial reports submitted to the EAC for they FY 2018 HAVA funds.

Some states such as Alaska, Arkansas, Delaware, Louisiana and Pennsylvania have used (or are planning to use) the full amount of the pre-CARES Act HAVA funds towards replacement of voting equipment, while others have used the funds for an assortment of election security measures. Below are examples of some of the ways individual states have been, and are planning to, use their allotted election security funds:

- **Arizona:** Efforts include replacing voting equipment; implementing a post-election audit system; upgrading election related computer systems; facilitating cybersecurity training; and implementing cybersecurity best practices.
- **Colorado:** Efforts include upgrades to the voter registration/election management system; incident response and preparedness training/exercises; vulnerability/penetration testing of election systems; improvement to risk-limiting audits; and security audits of election systems.
- **Connecticut**: Efforts include voting equipment replacement and upgrades; election cybersecurity training; enhanced password protection for election systems; IT infrastructure upgrades; post-election audit enhancement; and election security reviews.
- **Georgia:** Efforts include replacing voting equipment; conducting cybersecurity assessments; purchasing e-poll books; conducting election audits and testing; purchasing cybersecurity sensors; and improving voter registration database management and access control.
- **Indiana**: Efforts include expanding multifactor authentication statewide; establishing incident response resources; cybersecurity training; technology evaluations and email encryptions; and grants to counties.
- I**owa**: Efforts include hiring a Cyber Navigator; improvements to IT infrastructure; election security training; security upgrades to the voter registration system; implementing multi-factor authentication; conducting risk and vulnerability assessments; security upgrades to county websites/systems; transitioning county website domains to .gov.
- **Mississippi**: Efforts include grants to counties for election security activities; cybersecurity audits and training to counties; implementation of multi-factor authentication; developing post-election audit materials; and upgrades to the state election management system.
- **Nevada**: Efforts include implementing new security features for the state voter registration database; grants to counties for Albert Sensors; auditing of election procedures; election security training and exercises; implementing digital email certificates and multifactor authentication; and communication/education efforts.
- **Rhode Island**: Efforts including purchasing new voting equipment; upgrading the state voter registration system; implementing database activity monitoring and file system security; implementing asset management and appliance software; software assurance for database platform; purchase of a subscription server for application vulnerability scanning.
- **Washington**: Efforts include purchasing equipment to capture and monitor network traffic; establishing a Security Operations Center; implementation of multi-factor authentication; analysis/assessment of election systems; and election cybersecurity training.