Help America Vote Act (HAVA) Funding and Critical Infrastructure Security

Utilizing Grant Funding to Address the Top Concerns of State CISOs

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Critical infrastructure (CI) is the central nervous system of modern society. Citizens interface with multiple components of CI on a daily basis; power generation and distribution, water treatment, communications, and public transportation, among others. Interruption of these services - through structural failure or by a threat actor - for even a short period of time can have serious and wide-ranging effects on public safety and public health. Developing resiliency within this critical infrastructure is therefore a primary responsibility of all levels of government: federal, state, county and municipal. The US Department of Homeland Security (DHS), in response to Presidential Policy Directive/PPD 21 (2013), has designated 16 critical infrastructure sectors that must be covered in order to achieve this resiliency, and has promulgated policy directives accordingly. DHS added Election Infrastructure as a Critical Infrastructure Subsector in 2017. This designation raised the profile of elections security substantially. It also allowed states to integrate elections security into their existing critical infrastructure resiliency plans and to apply resources accordingly. In fact, DHS was empowered to engage in cross-sector collaboration and resource sharing as a best practice.

> ***"DHS (has) the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms are used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors."*** **-** Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience

In March 2018 President Trump signed the Consolidated Appropriations Act of 2018 into law. The Act included $380M in grants, made available to states to improve the administration of elections for Federal office, including to enhance technology and make election security improvements. The U.S. Election Assistance Commission is the administrator of the grant funding through the Help America Vote Act of 2002. This new funding was, in effect, now to be used to enhance the security of a DHS-designated critical infrastructure sub-sector. The HAVA funding may therefore – at the states discretion – be utilized to support the security of other, DHS-designated, critical infrastructure sectors.

> ***"HAVA expressly prohibits the EAC from issuing regulations of relevance to the CI designation, and it leaves the methods of implementation of the act's requirements to the states."*** **-** Title I, Section 101 of the Help America Vote Act of 2002

All eligible grantees requested their share of the HAVA funding prior to the 2018 mid-term elections. A plurality of 41 grantees estimated that they would spend at least a portion of their HAVA funding on cyber-related initiatives, accounting for roughly $134M of the $380M total funding. Another 21 states indicated that they would hold at least some portion of their grant funds in reserve, a total of over $54M. The flexibility of these reserve funds was made clear to the states in the FAQ section of the grant application.

> ***"The states have a great deal of flexibility in how they deploy the federal grant funds. The 'Reserve' category…are for funds that have not yet been budgeted by the States. As needs or threats become apparent the funds designated in Reserve will move to other categories…"*** *HAVA Election Security Funds Q&A*

It is clear that states have broad discretion with regard to how they use their HAVA grant funding to support their election security efforts. It is also clear that the use of these funds is not limited to any one CI sector or subsector. The spending category most oft-cited by states for HAVA grant funds - "cyber security" - can therefore be used to enhance cyber security across all critical infrastructure categories. Creating a reserve, the second most-cited spending category, can be used for similar purposes or to create a dedicated cyber security budget in the 41% of states that currently lack such funding.

> ***"Almost half of states do not have a separate budget line item for cybersecurity"*** - 2018 Deloitte/NASCIO Cybersecurity Study

Finally, the states also have flexibility with regard to what is considered part of "election infrastructure". A number of databases containing citizen data interface with election systems year-round, and not just during an election. Departments of motor vehicles and corrections, and secretaries of state are among a number of possible interfaces to voter records and election infrastructure. Each of these interfaces brings with it increased potential access for threat actors. States should look at all of these interfaces as part of a "living, breathing" election infrastructure that must be protected 24/7/365. Utilizing HAVA funds designated for cyber security – or reserve funds without designation –to address potential vulnerabilities can extend the impact that these funds have on all citizens.

II. ELECTION SYSTEMS AS CRITICAL INFRASTRUCTURE

Critical Infrastructure Defined

The term "critical infrastructure" (CI) is defined in the *Patriot Act of 2001* as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". *Presidential Policy Directive 21 – Critical Infrastructure and Resilience*, published in 2013, designated sixteen critical infrastructure "segments". Election infrastructure was designated as part of critical infrastructure as a subsector under the Government Facilities sector in January 2017. This designation was the result of FBI investigations of cyber attacks that took place during the 2016 presidential election.

Election Systems Critical Infrastructure Components

"Election Systems" go beyond the equipment necessary to record and capture individual votes. It also includes the IT systems that properly register a voter, as well as the systems used to report the results of an election. This definition is necessarily subjective, since each jurisdiction responsible for the election process will have its unique circumstances, including the number and types of interfaces that are required for these systems. The result is a short, but broad list of what is included under the definition of "Election Infrastructure".

Election Infrastructure includes <u>but is not limited to</u>:	
1	Voter registration databases and ***associated IT systems***.
2	***IT infrastructure and systems*** used to manage elections (such as the counting, auditing, and displaying of election results.
3	Voting systems and associated infrastructure.
4	Storage facilities for election and voting system infrastructure.
5	Polling places, to include early voting locations.

Notable Consequence of the Critical Infrastructure Designation

A notable consequence of the designation of election systems as CI is that DHS has the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms can be used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors. This means resource sharing among CI sectors and subsectors is encouraged. The logical extension of this funding would be for tools that can be used across the CI sectors and subsectors.

State National Guard Units and Critical Infrastructure

Title 32, Chapter 9, of the United States Code gives governors the ability to utilize their state's National Guard units for "homeland security efforts ". This term refers to "an activity undertaken for the military protection of the territory or domestic population of the United States, ***or of infrastructure or other assets of the United States*** determined by Secretary of Defense as being critical to national security, from a threat or aggression against the United States.

III. 2018 HAVA GRANT AND ELECTION SYSTEM SECURITY

Funding Authorization and Utilization of Funds

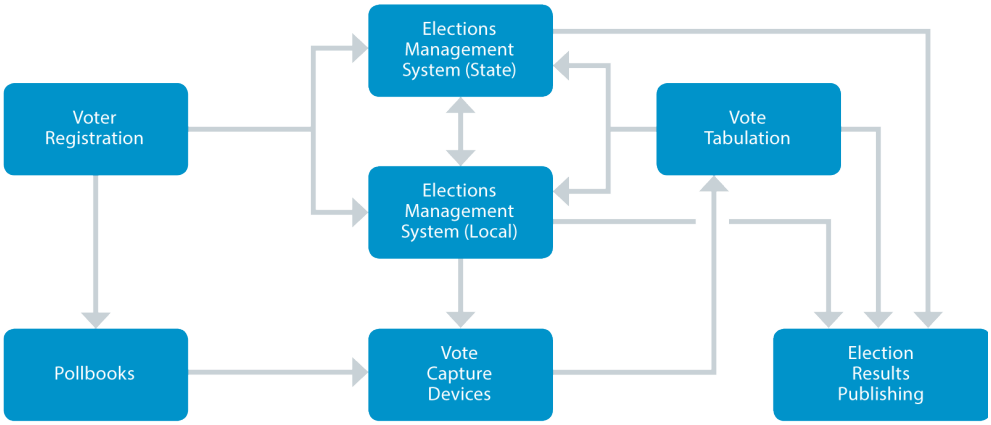
The Consolidated Appropriations Act of 2018 provides $380M to the Election Assistance Commission to make payments to states for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements, as authorized by the Help America Vote Act (HAVA) of 2002). The Act included $380 million in grants, made available to states to improve the administration of elections for Federal office, including enhancing technology and to make election security improvements. In essence, the HAVA funding is now available to support a critical infrastructure sub-sector.

States may use the 2018 HAVA funding to:	
1	Replace voting equipment that only records a voter's intent electronically with equipment that utilizes a voter-verified paper record.
2	Implement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally.
3	Upgrade ***election related computer systems*** to address cyber vulnerabilities identified through Department of Homeland Security, or similar scans or assessments of, existing election systems.
4	Facilitate ***cybersecurity training*** for the state chief election official's office and local election officials.
5	Implement established ***cybersecurity best practices*** for election systems.
6	Fund ***other activities*** that will improve the security of elections for Federal office (CI).

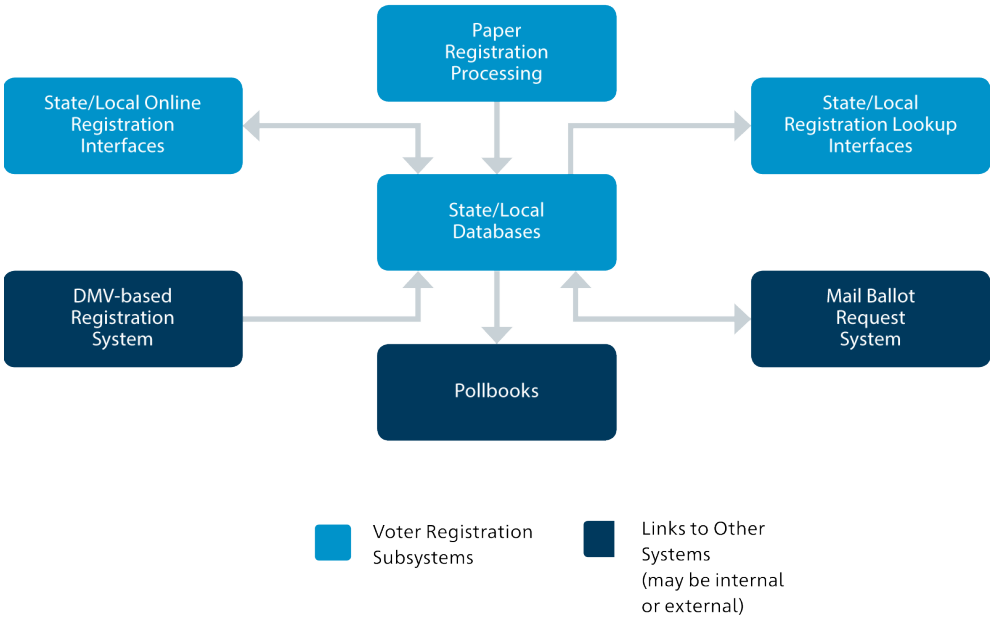
These six categories again highlight the flexibility of HAVA funding once it is in state hands. The word "may" in the heading is critical because it offers states the option to potentially use the funding for other purposes, with the caveat that it be relevant to securing election infrastructure. Had this heading used "shall" instead of "may" states would have been severely limited with regard to how they use the funds. This does not appear to be the case, which is consistent with the overall discretion given to the states for managing these grant funds. The last four of these six categories are of particular interests for states because all four can be used to increase the value of the HAVA grants by extending them beyond "election infrastructure".

Election-Related Computer Systems

The generalized election system architecture represented below is fairly consistent across the states and appears to be fairly self-contained. However, data is not contained solely within voting machine hardware, and vote tabulation and reporting data is often moved over networks that are administered by non-governmental entities. Combine this with proprietary software that may or may not have the most recent patches installed and there remains a real possibility that a threat actor could gain access by way of a zero-day vulnerability that would exist solely in the process of conducting an election. States should therefore have a robust vulnerability capability in place and run scans on a regular basis in off-election periods to ensure that a vulnerability does not exist on the day of an election.



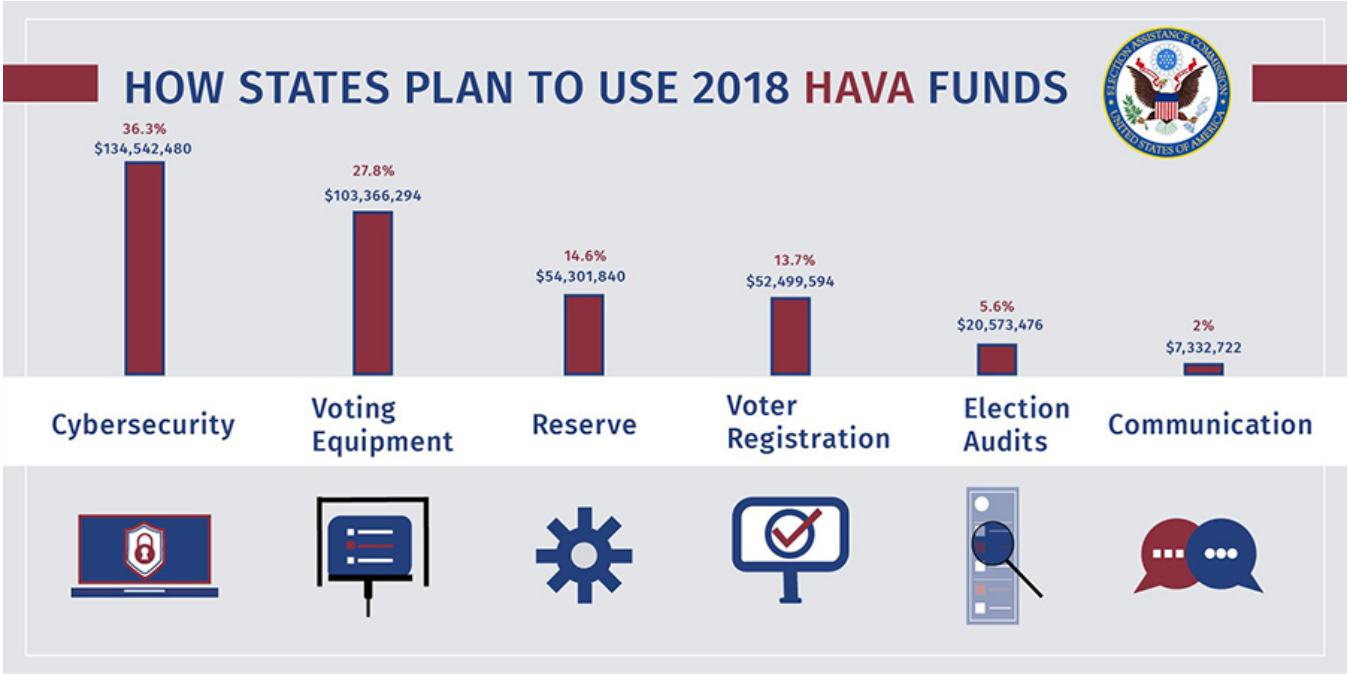
Acquisition of a vulnerability management solution to address this security issue is clearly within the HAVA guidelines. Based on an expanded definition of an "election-related computer system" that includes all the interfaces to the system, the same vulnerability management solution may also be used to cover all of the systems connected to the election system through those interfaces. As an example, take one component of a traditional election system – voter registration. The figure below presents the high-level architecture for a voter registration system, clearly identifying "state/local databases" as the center of this critical component while also acknowledging that several interfaces to these databases may come from external sources, providing additional gateways for threat actors to enter the election system. This would certainly support the use of HAVA funding to expand the use of acquired cyber security tools to also cover these external interfaces.



State Priorities for HAVA Funding

The Election Assistance Commission polled the states regarding their priorities for the 2018 round of HAVA funding. The graphic below presents their responses across six broad categories. The highest percentage of states (36%) responded that they would spend their grant funding on "cyber security". This was higher than those who said they would be replacing voting equipment (27%). Initially it was thought that the replacement of outdated voting machines would be the primary use of this grant funding, and many elected officials pointed to the machines themselves as the culprit for the perceived work of threat actors during the 2016 election cycle. Interestingly, the third most common response (14%) was "reserve". These results all stem from a miscalculation

on the part of the EAC regarding how states acquire, implement, and test voting system enhancements. The results also revealed, of the 23 states and territories that indicated at least part of their funding would go to "reserve", 20 were also part of the group of 41 states who indicated they would spend on cyber security.



There are at least three reasons for this distribution of responses

1. ***States did not have enough time to complete the procurement processes required for the acquisition of new voting equipment***. With few exceptions, states approve election systems vendors, but the counties select the vendors. Thus, the funding at the state level must be distributed to counties, which then each have their own purchasing guidelines. There just wasn't enough time to spend the money in 2018.
2. ***Cyber security was a significant issue in 2018, but not as it relates to voting machines. Voting machines are closed systems and simply collect data***. The data transfers that take place before and after the actual collection of the vote – registration, poll book generation, tabulation, and results reporting – are where vulnerabilities lie, and states responded with those concerns in mind.
3. ***The states are focused beyond 2018.*** The projected cybersecurity spend plus the projected reserve accounts for almost half of the $380M in total grant funding allocated, which suggests that states were looking beyond 2018 when the funding was distributed. The 2020 presidential elections looms large for states, but three states – Kentucky, Louisiana, and Mississippi – will elect governors in 2019, and mayoral elections will be held in major cities, including in Chicago and Houston, two of five largest cities in the United States.

IV. Summary and Recommendations

The CISOs from all 50 states responded to a survey that produced the *2018 Deloitte-NASCIO Cybersecurity Study*. The top three responses to the question "Identify the top barriers that your state faces in addressing cyber security challenges" were the same as in the previous four editions of the study:

- ***Lack of Sufficient Funding/Lack of Sufficient Cyber Security Budget.*** 41% of respondents indicated their state did not have a dedicated cyber security budget.
- ***Inadequate availability of security professionals.***
- ***Increasing Sophistication of Threats.***

Though not a panacea, the designation of elections security as a critical infrastructure (CI) sub-sector, and the funding available to states via the Help America Vote Act (HAVA) to protect this subsector, can directly impact all three of these issues. The designation as CI provides the impetus to share resources between the Election

Systems sub-sector and other CI sectors. HAVA funding is designated for improving election system security, which is now part of CI security. States have broad discretion in both the definition of "election system" and in the utilization of HAVA funds to address their state-specific security challenges. The majority of states have indicated a predilection to spend these funds on cyber security solutions and training, which can be utilized for the entirety of state government, creating stronger coordination between entities and more effective response to threats. "Reserved" HAVA funding is flexible, and can be used at the states' discretion, when "threats become apparent" and priorities become clearer, regardless of which CI sector or sub-sector is affected.

Recommendations Regarding Critical Infrastructure and Elections Systems Security Funding	
1	Utilize HAVA funds to acquire cyber tools and solutions that can be shared across ALL critical infrastructure subsectors, per DHS directives regarding the facilitation of cross-sector coordination and resource sharing.
2	Adopt a broad definition of "election system" to include all the systems that interface with voter registration, vote capture and tabulation, and election results systems, and utilize standardized tools acquired with HAVA funds to cover ***all*** of these systems.
3	Create a separate cyber security budget line item utilizing the flexibility granted by the Consolidated Budget Appropriations Act of 2018 as it pertains to retained HAVA funds.
4	Establish standardized cyber security training modules – using standardized tools - across all state agencies, higher education, and the National Guard. This will enhance the ability of cyber security professionals to operate across these domains, increase the qualified talent pools available to state government, and enhance coordination during homeland security events

V. Tenable Solutions

Industrial Security

Industrial Security™, in concert with Nessus Network Monitor™ (NNM) sensors, delivers continuous asset discovery and vulnerability detection for safety-critical operational networks. Purpose-built for OT systems, the solution uses NNM passive monitoring to provide safe and reliable insight – so you know what you have and what to protect. Covering a wide range of ICS, SCADA, manufacturing, and other systems, Industrial Security helps IT and OT security, plant operations, and compliance teams enhance security, improve asset protection, and strengthen regulatory compliance. The OT-native solution provides an up-to-date view of systems, applications, and vulnerabilities to help organizations understand their OT cyber exposure and protect operational performance.

Features and Capabilities for Converged IT/OT Systems

- Support for thousands of OT systems from dozens of manufacturers, including Siemens, ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, and Schneider Electric
- Supported OT protocols include BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 61850, IEEE C37.118, Modbus/TCP, OPC, openSCADA, PROFINET, Siemens S7, and more
- Support for a wide range of IT assets, including servers, desktops, laptops, network devices, web apps, virtual machines, mobile, cloud, and containers

Tenable.io

Tenable.io, a cloud-based cyber exposure platform, helps organizations manage risk on IT networks connected to OT networks in converged IT/OT systems. Tenable.io Vulnerability Management active and agent-based Nessus™ sensors discover and thoroughly assess the full range of on-premises and cloud-based IT assets. Tenable.io's active Nessus scanner can easily be configured to not scan specific port and/or IP addresses.

Tenable.sc

Tenable.sc (formerly SecurityCenter) is a market-leading vulnerability management solution that provides real-time, continuous assessment of your security and compliance posture across your entire IT infrastructure, actionable insight into prioritized weaknesses and continuous assurance that security and compliance are aligned with organizational goals. Like Tenable.io, its active Nessus scanner can easily be configured to not scan specific port and/or IP addresses.

VI. About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver Tenable.io®, the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 20 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
North America +1 (410) 872-0555
www.tenable.com