How to Solve Election Day Cyber Threats

Anyone in the United States (US) who is exposed to media outlets cannot help but be barraged with articles about election tampering both in the past and potentially in the future. This alleged tampering happens as social media influence and hacking the integrity of the voting process. As a Cybersecurity strategy practitioner, I find this fascinating that people feel like we can't believe this has happened or could happen again. But, I take a step back and look at the state of our country, both in the Cybersecurity and the Election Landscape and apply US human behaviors; then I can see why we are where we find ourselves. The reality is, we have the answers to solve these problems, we just choose not to observe them. As, Sir Arthur Conan Doyle's character Sherlock Holmes states, "It is not to see, but to observe!" As I said, the answers to solve this problem are in front of us. Let me help you observe……

First, what are our elections processes? The US is so worried about election integrity for our democratic republic that they have created an office to be the national clearinghouse of election information. That office, The US Election Assistance Commission (USEAC) (www.eac.gov), is charged with helping to ensure the execution of the Help Americans Vote Act of 2002 (HAVA). Since there is also considerable turmoil in interpreting the Constitutional Rights of the states in the election process, we have created a situation where the US is paralyzed in understanding procedure and that inhibits our ability to address the Cybersecurity threats against the electoral process. Further, the US has many jurisdictions (county, state, Federal) that govern over their respective elections procedures for voting creating a jurisdictional maze. So, what are we to do? Just look at each other as time flies by? I say there is a way to ensure the voting integrity of election days throughout the United States. What is that approach? It is the EigenVote Framework.

What are the components of the EigenVote Framework? It is an approach that leverages the Cybersecurity Awareness and Resiliency (CAR) tenets, the Cybersecurity Landscape Ontology and Taxonomy (CSLOT) organized approach, the Cybersecurity Order of Operations Methodology (COoOM) to understand required security controls, NIST NICE Cybersecurity Workforce Framework (CWF) for properly trained personnel, NIST Cybersecurity Framework (CSF) for categorizing process and understanding Cybersecurity Impact, Office of Management and Budget (OMB) Circular A-130 and associated guidelines/memorandums to ensure alignment to National level protections, all Privacy standards (Privacy Act, Controlled Unclassified Information [CUI]), NIST SP 800-160 Volume 1, System Security Engineering considerations, NIST SP 800-160 Volume 2, Cyber Resiliency Considerations, NIST SP 800-53 Rev 5 to ensure proper selection of security controls, and all Federal Cybersecurity statutes. This sounds like a quite a bit and it might even be daunting to understand how all this comes together. Let's dig in a little more, shall we?

The EigenVote Framework focuses on the following major building blocks:

I. Adopt the CAR tenets
II. Establish "Election CISO" role
III. Institute the CSLOT approach
IV. Leverage the COoOM for security control selection
V. Layer other jurisdictional impacts as appropriate
VI. Adopt NIST SP 800-160 and SP 800-160vol2 to create a systems design with Secure principles and Resiliency
VII. Implement the Federal Election COoOM result architecture
VIII. Update all election processes to ensure they do not violate I-VII above

First, to execute the EigenVote Framework at any voting jurisdiction, we recommend every Voting Jurisdiction create a specific role focused on executing the EigenVote Framework. This role could be called "Voting CISO" or "Election CISO" for a given jurisdiction. This is where the NICE CWF provides guidance for us. See CWF for an explanation of this type of role:

> *Oversee and Govern (OV), Executive Cyber Leadership (EXL), Executive Cyber Leadership, OV-EXL-001 Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations*

So, if we continue to use the CWF, we can now have a job description, certifications, experience, education and the Tasks, Knowledge, Skills and Abilities required for this job. See my article in LinkedIn called "What does a CISO look like now?" (https://www.linkedin.com/pulse/what-does-ciso-role-look-like-now-aaron-bishop/) to understand all these important aspects of the role. The important part of an Election CISO is that it MUST follow the tenets of the CAR. The Election CISO should report to the top Election Official of the corresponding jurisdiction. The Election CISO should not only have a voice but have the definitive voice regarding Cybersecurity. The Election CISO should be empowered to make any decision necessary to ensure the Confidentiality, Integrity, Availability, Criticality, Privacy and Assurance of the Voting process without being overridden by anyone in the organization for the sake of expediency, cost or convenience. Per the tenets of the CAR, if someone overrides the Election CISO on these decisions, they have violated the CAR, and possibly a legal statute. Following the CAR prevents anyone from knowingly, unknowingly, wittingly or unwittingly affect the Cybersecurity posture and integrity of the voting process.

Now that we have an Election CISO driving the CAR throughout the process and jurisdiction, we now need an approach to ensure comprehensive Cybersecurity. That is the Cybersecurity Landscape Ontology and Taxonomy (CSLOT - www.eigenspace.us/docs/CyberSemantic.pdf). This process begins by understanding ALL the stakeholders and requirements levied against the mission. What statutes apply, what standards apply, what requirements apply are just a few examples of the awareness required by the Election CISO. This approach helps to ensure that they are all accounted for. Additionally, this approach systematically ensures everything in Cybersecurity Lifecycle is addressed. The architecture, the vulnerabilities, the security controls, etc. are all levels within the CSLOT to ensure comprehensiveness. A most neglected area of Cybersecurity that the CSLOT ensures is the evidentiary based assessments of security controls. This is legal proof that the voting jurisdiction did what they were expected to ensure privacy and assurance to the Federal standards and statutes. This evidentiary approach is necessary should there be ANY challenge to the voting process. By following this approach, you now have legally defendable evidence to prove the process was followed properly assuring the integrity of the voting process.

Level 3 of the CSLOT is the Cyber Order of Operations Methodology (COoOM). This specific process is a powerful litmus test to ensure all requirements, stakeholders, regulations, statutes and intended outcomes are accounted for in a scientific manner removing human bias when selecting Cybersecurity controls. The process of Cybersecurity control selection is usually rife with human bias because of arbitrary checklists, vendor or organizational standards, compliance instructions or risk-based decisions all made without understanding the impact of de-selecting these controls. A scientific approach to ensure that the proper controls are selected and de-selected is the key to understanding if you have met your intent of the voting process: an untampered collection of votes from properly identified voters of a jurisdiction. By using this approach, the removal of single Cybersecurity control can be evaluated to ensure no unintended negative impact to the overall solution is inherited (known or unknown). The EigenVote Framework, has a layered approach to this problem. By using this scientific approach, Eigenspace has identified the Federal Voting Baseline of security controls required. Additionally, you can modularly layer on which state required controls are needed to create a unique State Voting Baseline for each state. This process can continue down further to smaller jurisdictions all the way to polling stations. The result is the EigenVote Framework can scientifically identify all required Cybersecurity controls for voting regardless of jurisdiction (thus eliminating the jurisdictional paralysis we observe today).

Today, we constantly are inundated with vendors both with niche Cybersecurity products or Cybersecurity Consultancies providing best practices and approaches that are based on narrow focus areas that have human bias permeating throughout their approaches and products. The issue we keep ignoring is the truthful answer, placing Cybersecurity has the anchor system design requirement and building solutions from that point of view. We don't. We build disparate systems with nothing but a focus on "speed to market", "mission imperatives", "cost management", "risk management decisions", or consumer "instant gratification". Then we, as Americans, are stunned when these solutions violate our data's integrity, and have no protections? BUT, we have answers to these problems if we only observe. NIST has created the SP 800-160 Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems and the SP 800-160 Volume 2, Draft, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. By starting over with the systems design for voting by the Election CISO, organizations can ensure they have addressed Trustworthy tenets and Resiliency in their voting systems.

Another area that needs to be understood is the architectural approach to establishing the information systems in support of this process. Instead of taking a human-biased best-practice approach, a vendor specific architecture (where you inherit the vendor's human-bias), or, worse, a legacy architecture perspective, why not do something more scientific? We can now use the resultant requirements from the CSLOT (regulations, statutes, COoOM results, trustworthy system design, Cybersecurity Resiliency and evidentiary requirements) to drive the architecture. By using these known control baselines, tenets and approaches, we can compare products and the security controls that they mitigate. This creates an architecture that ensures you haven't missed a security control and eliminate human biased decisions, Cybersecurity holes in architectures through vendor approaches, and an architecture that meets the evidentiary based requirements that today's approaches just don't meet. Eigenspace has already created such an architecture that meets all these parameters. I am confident that if the EigenVote Framework is leveraged, voters can be confident their voting process integrity will be intact. The only thing jurisdictions must worry about would be "fake news" and undue influence of voters outside of the voting process and not vote tampering.

How to Solve Election Day Cyber Threats

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us