Locality Minimum
Cybersecurity Standards

NASED Winter Conference

Christopher Piper
Commissioner
chris.piper@elections.Virginia.gov
804-864-8903
Elections Security for the Commonwealth is essentially three-fold:

• **Virginia Information Technology Agency (VITA)**—securing the perimeters, networks and servers
• **ELECT** — securing the Voter Registration software application, data & system access
• **Localities** — securing the local electronic pollbooks, voting equipment & Registrars’ endpoint devices *(for accessing the central Voter Registration system)*

**HB2178** – Is the means for the Commonwealth to **improve locality security maturity** through:

• Establishing minimum security standards & plans
• Gaining improved visibility of Locality security risks, and
• Influencing timely mitigation
Locality & Department of Elections (ELECT) Workgroup / Team

“... in consultation with representatives of local government information technology professionals and general registrars, update the security standards at least annually.

Such review shall be completed by November 30 each year.”
**HB2178 / § 24.2-410.2**

**ELECT must:**

- Ensure security & integrity of Virginia voter registration system and the supporting technologies utilized by counties & cities to maintain and record registrant information.

- **In consultation with** representatives of local government information technology professionals and general registrars, update the security standards at least annually. *Such review shall be completed by November 30 each year.*

- Ensure the electoral board of each county & city:
  - Develop & annually update written plans and procedures to ensure security & integrity of those supporting technologies
  - Be in compliance with the security standards
  - Report annually by March 1 on its security plans and procedures

- Ensure the general registrar & ELECT report annually on their security plans & procedures.
Locality Elections Security Challenges

1. Differences in locality security maturity, including Risk Management, Information Security Planning & Program Management
2. Lack of resources (i.e. people, process, technology, financial, knowledge)
3. Localities were asked to implement standards & plans prior to funding decisions, and leading into and throughout a National Election calendar year; Security Plan due by March 1, 2020, and a risk assessment needed to be completed prior to that. Thus, working as best possible to roll out in a phased approach, and using quantitative analysis/metrics to lobby for funding.

Designing, implementing and maintaining a risk-based information security plan & program is crucial to maturing information security and gaining the right funding support for initiatives.

**Foundationally, an Enterprise Information Security Plan would contain at a minimum:**
- Information Security Strategy & Governance Framework
- Information Risk Management *(not System Risk Assessment)*
- Information Security Program Development & Management
- Information Security Incident Management*

**With the 6 basic outcomes of:**
- Strategic alignment
- Risk management
- Value delivery
- Resource optimization
- Performance measurement
- Assurance process integration

* Encouraged the NGA Policy Academy to assist with sharing existing policy, plans, processes and highest risk “election cybersecurity” related scenarios that localities and states should address in plans
Locality Elections Security Challenges (cont.)

System & Services Acquisition & Maintenance Standards related to Electronic Pollbook & Voting Equipment: [Even though technically out of scope of HB2178, these are security concerns states are struggling to address!]

1. Vulnerability Patching & Software Updates * (requires a recertification process)
2. Procurement Security Requirements ** (localities don’t have experience to know what to ask for)

* Due to the costly and/or lengthy recertification processes, vendors are either not: patching, applying timely vulnerability patches, and/or performing appropriate system testing thereafter.

** Procurement Managers within localities wield power; some simply won’t comply. Others don’t have the knowledge to craft appropriate contract language, etc.

Additional areas the NGA Policy Academy could assist with, as these are nationwide issues/challenges:

- Different recertification tiers – i.e. for initial certification vs. vulnerability patching updates, etc.?
- Sample contract language for procurements of equipment, best practice level of maintenance & SLAs?

**NOTE:** CIS published Election Technology Procurement Guide in May 2019.
- Make vendors fully accountable for timely maintenance of their system with IT performing oversight?
Work group / Team Collaboration

- HB2178 was very prescriptive as to the make-up of the work group of individuals that were to be assembled
  - Work group:
    - Locality IT & Security professionals; varying from rural, urban, small, medium, large
    - General Registrars
    - Joint Legislative Audit Review Commission (JLARC) representative
- The Work group was chaired by the Department of Elections (ELECT) CIO

Additional individuals were invited to attend the meetings to include their perspectives
  - VML representative (Virginia Municipal League)
  - VaCO representative (Virginia Association of Counties)
  - Additional ELECT participants
  - Additional Locality IT & Security professionals
Work group Charter / Goals

Through a series of seven 4-hour sessions from late May through early October, the HB2178 prescribed work group met every 3 weeks with the following goals:

• Promote security standards and improvement of locality security posture
• Review security standards and provide:
  – Recommendations for approval of standards
  – General cost estimates for implementation of such security standards
  – Evaluation of the risk of not implementing certain industry standards for localities
• Provide recommendations to achieve security of the Virginia voter registration system and the supporting technologies utilized by the localities to maintain and record registrant information
Approach

The Locality Security and Operations Minimum Security Standards & Plan Templates were developed utilizing best practices and resources from various nationally recognized election & information security federal and state agencies and frameworks, and not limited to:

- Department of Homeland Security (DHS)
- U.S. Election Assistance Commission (EAC)
- National Institute of Standards and Technology (NIST)
- Center for Internet Security (CIS) Top 6
- Virginia Information Technology Agency (VITA)

Approach:

- One that will result in “Defense in Depth” (depicted to the right)
- Standards & Plan Templates are written rather generically, to help localities easily apply to other systems outside current scope; will call out some specifics related to elections, though generally not tailoring standards specifically to the HB 2178 scope, rather in alignment with NIST Cybersecurity Framework and NIST 800-53 controls, etc.

Note: The term Information Security includes Privacy
Recommendation

While localities are being asked to implement standards and plans prior to funding decisions, the work group supported the recommendation of these minimum security standards as being “the right thing to do”.

The recommendation was made in good faith, that:

- Funding assistance would eventually be provided to localities
- ELECT would not cut off a locality’s access to the Voter Registration System as long as the locality:
  - Had communicated their mitigation plan
  - Is working in partnership with ELECT
  - Is making continued progress in alignment with the plan.
Standards Implementation Timeline

Work group: “Prudent for localities to at least be compliant with those standards identified as Critical & High by September 1, 2020”.

Though the General Cost Estimates to implement the standards was a small sampling (9 of 133 localities), analysis showed:

- Size of locality does not necessarily imply greater elections security maturity
- Elections security maturity, even to these minimum standards, varies greatly

Experience shows:

*It is a tall order to deliver upon, and most especially in a National election year and when funding has not yet been approved/provided.*

- Likely difficult for localities to fully implement the 7 Critical and 10 High risk priority minimum security standards by September 1, 2020
- *Some success in improving security maturity is better than none!*
Next Steps

• December 31, 2019, localities were required to complete:
  – A Risk Assessment: The NCSR & EIAT Baseline Self-assessments
  ELECT established a HB2178 Support Team and continues to assist localities

• March 1, 2020
  – Localities review Risk Assessment, Security Plan & Minimum Security Standards Complaince Checklist with locality GR & Electoral Board in closed session
  – Electoral Boards submit Minimum Security Standards Compliance Checklist to ELECT & confirm their annual review of the locality security plans and procedures

• September 1, 2020
  – Critical and High Priority fixes must be implemented

_ELECT is currently analyzing the results to gain a better understanding of risks, and to develop mitigation strategies; short term & longer term._
Thank You

Questions?

Christopher Piper
Commissioner
chris.piper@elections.Virginia.gov
(804) 864-8903