"Revisioning the U.S. Elections Process: Voting Security and Election Integrity"

Georgia Institute of Technology[1]

June 3, 2019

Abbreviated Version
Prepared for 2019 NASS Summer Conference
Complete Report Can Be Found Here

1.0 Introduction: Revisioning the U.S. Elections Process: Voting Security and Election Integrity

Concerns about the overall integrity of the U.S. electoral system have been raised in light of recent events including the perceived (and real) vulnerabilities of voting technologies. This paper 1) identifies key security policy challenges facing elections officials and 2) proposes a comprehensive General Model for Voting Security (GMVS) as part of an Independent Assessment Framework (IAF) intended to address many of these concerns.

2.0 State of U.S. voting systems and voting technology: Key Issues

An aging and complex national electoral infrastructure challenge voter security perceptions, confidence and trust in the integrity of the electoral system. Certification of systems provide a certain level of confidence that the systems will work as intended, and addresses *basic* security issues, but can have the undesirable effect of inhibiting broad innovation of new systems, as well as security related approaches[2].

Key challenges include:

1) *Ease of Assessing Security*
2) *Effectiveness of Security Assessment*
3) *Target and Appropriate Communication to Various Stakeholders*
4) *Usability/accessibility processes, workflow and communications as well as just technology*

3.0 Critical System Elements: Technological Security, Policy Considerations, and Communications

Conceptual aspects of security

Traditionally, election security has focused on encryption, digital signatures, protection of voting information, facilities, and events. A common misconception is that **hackable voting technology,** is the weakest link in the election process, but in reality, the most problematic security problems come from software bugs, or errors in processes. This underscores the importance of a robust communications and outreach/engagement strategy to counter public and other media driven misconceptions. Election officials need to assess and secure the electoral process including technology, related government functions such as handling and operation of the voting workflow; and external functions that touch the entirety of the elections process: procurement, staffing, and vendor management. Security is not simply at the physical and technology/access level, but includes the integrity of the entire voting process. The 2018 NASEM report, *Securing the Vote: Protecting American Democracy* observed: "There are numerous ways in which the integrity of elections can be affected."

---

[1] For more information, or to comment on this paper, contact Paul M.A. Baker, Ph.D., Georgia Tech, [paul.baker@gatech.edu]. We acknowledge the support of the Smartmatic Corporation in conducting this research.
[2] University of Pennsylvania (2016)

Policy and regulation tend to be developed in a reactive manner in the U.S., frequently in response to technological advances and events which draw public awareness. While, a voting system compliant with the EAC's Voluntary Voting System Guidelines (VVSG) 1.1 is not necessarily a totally secure system, in that the focus of VVSG 1.1 is not *primarily* security, and provision of (Federal) resources only addresses part of the problem.

4.0 Critical System Approaches: Assessment and election audit/evaluation tools

Technology, voting processes, and overall election management are subject to security and risk assessment (Darnolf, 2018) on the front-end, as well as ongoing monitoring and audits during and post-election (NASEM, 2018). Effective election security involves implementing a set of proactive processes grounded in an empirical, fact-based conception of physical security, that considers interaction effects of system level security variables, and is aimed at overall voting system integrity. Such an approach currently under development by the Georgia Tech Research focuses on development of a refence model: *General Model for Voting Security (GMVS)*, designed to evaluate election integrity.

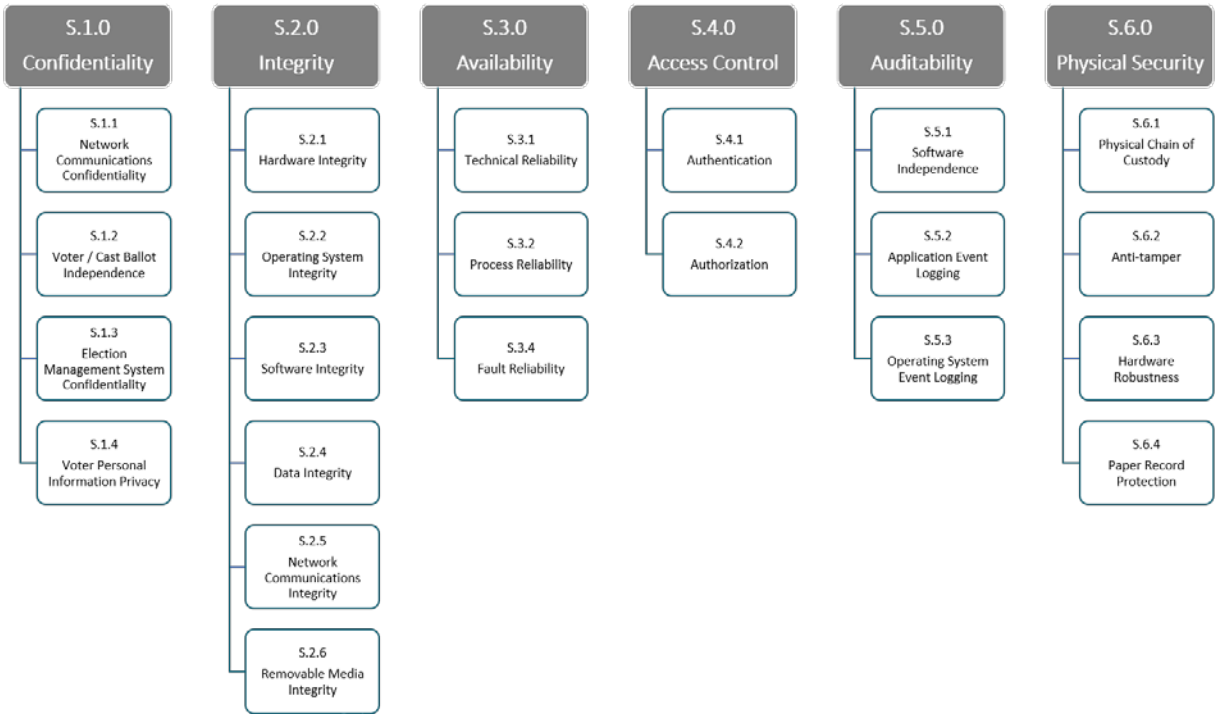

Figure 1 - *General Model for Voting Security (GMVS)*

In addition to the GMVS, an Independent Assessment Framework (IAF) outlines the independent process of assessment in order to evaluate security early on from the design phase. The framework assumes that an independent agent (in yellow, Figure 2, below) will provide the reference for the assessment (the GMVS in this case) and that agent will assess security first at design, then at implementation, and then at production.

The approach as outlined below, is based on a 1) requirements component, 2) a threat component, and 3) security component, detailed below.

The **Requirements** component for a general voting system is weighted toward factors particularly impacted by security – the physical components and overall electoral process. Additional elements include the need for voting equipment to meet standards and requirements (including accessibility and usability objectives), cost to *acquire* and *maintain* equipment, timely vendor support, and strategic considerations, such as overall performance/features and longevity of voting equipment.

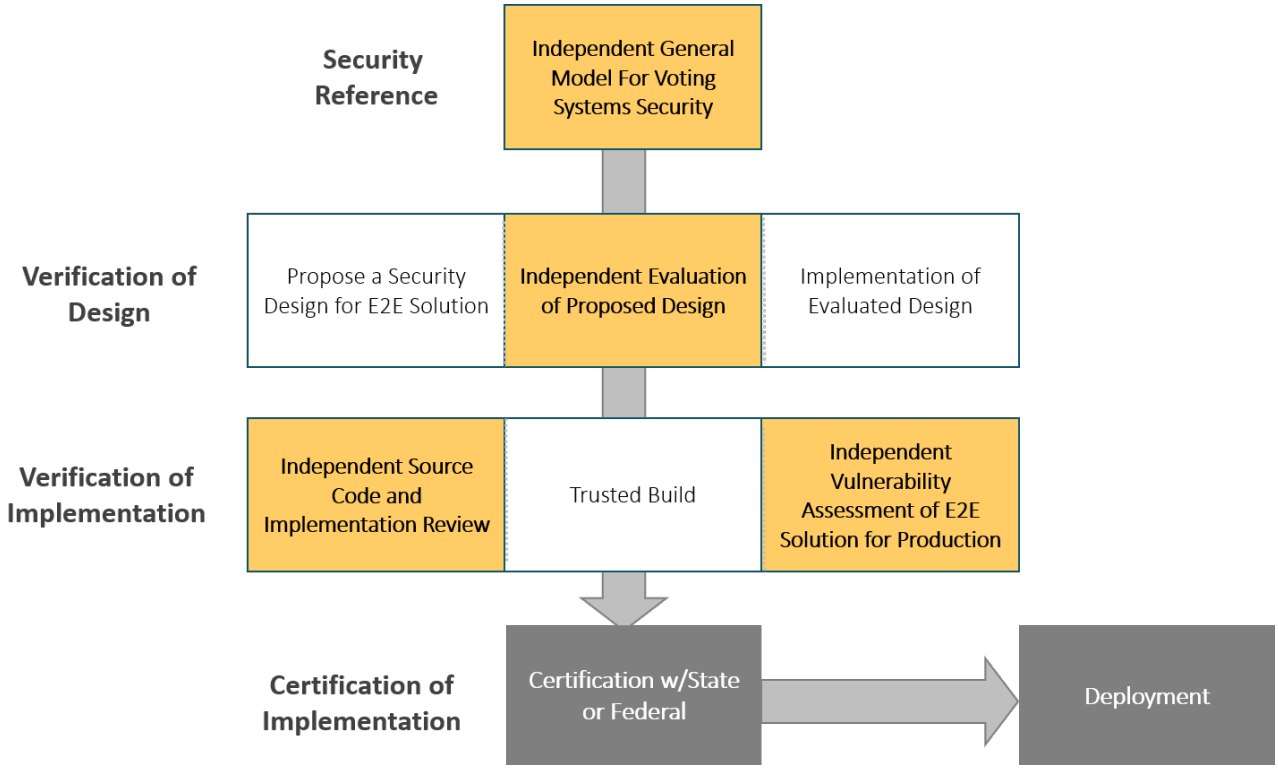

Figure 2 – ***Analytic Framework for Assessment (Independent Assessment Framework)***

The **Threats** component is a systematic description of the ways that an attacker could attack a system. Part of the difficulty in creating a secure system is that not all threats can be anticipated. Therefore, the importance of having a comprehensive threat model, with an end-to-end scope allows structural consideration of possible attacks, and to build a protection model accordingly, based on layered defenses.

The **Security** component is derived from consideration of the general requirements of a voting system in an adversarial setting. The security requirements are a means to protecting an election, whereas the main requirements model is the end itself.

Figure 3 (below) provides a conceptual illustration of the benefits of this approach. The two axes capture dimensions of certainty (assurance of security) and implementation (capacities, complexity of implementation cost). Given the complexity and many aspects of security, how can a jurisdiction be sure that the various options actually account for, and provide the security needs of the local voting process?

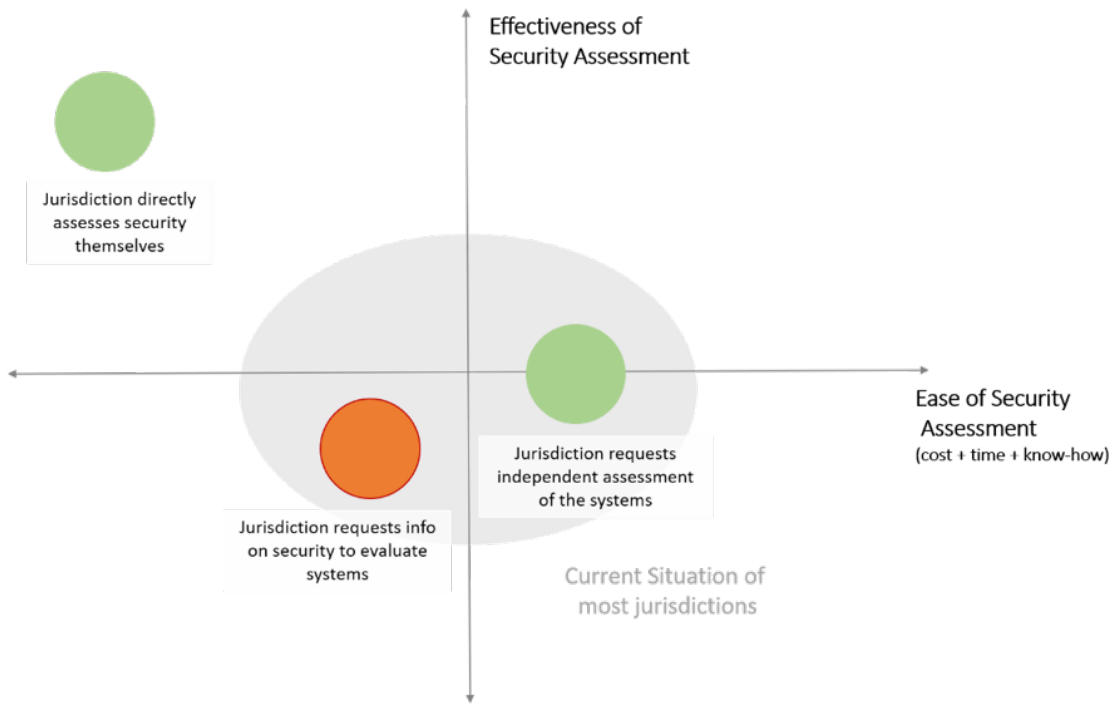

Figure 3 General Model for Voting Security and Independent Assessment Framework Approach

In theory, a jurisdiction issues requests to vendors for system (lower left quadrant). In practice, jurisdictions default to asking vendors to explain their security, which is low on the *Assurance of Security* axis, because vendors may not disclose security flaws of their systems.[3] This approach also scores low on *Ease of Assurance* as security descriptions may not be standard.

Jurisdictions also have a need for vendors to independently assess parts of their systems (middle right to the center quadrants). And if the RFP has no specific approach defined, vendors may selectively test some parts of their systems to comply with the *stated* tender requirements. In reality jurisdictions may: 1) "not pay" for assessment, specifically, 2) not invest time as a required deliverable to tender, 3) simply rely on vendors statements that security is adequately provided for.

The proposed model consists of an independent external comprehensive security review, with a jurisdiction requesting that vendors independently assess their systems based on an E2E independent model (Upper right corner). It scores high on the *Assurance of Security* dimensions, because an independent entity conducts the full E2E assessment of the system rather than a de minimis, set of selective penetration tests on *parts* of the system. Cost savings occur if all jurisdictions follow this standardized process, which has aggregated benefits by avoiding redundant independent assessments, hiring of consultants; and for vendors, this approach minimizes the need to have the same system to be evaluated multiple times with minor differences. If vendors do it once, the cost is "distributed" across all jurisdictions, and compliance with the independent assessment based on the same model, allows jurisdictions to easily compare options.

[3] Dunn & Merkle (2018)

5.0 Innovation and New Approaches to Electoral Process Integrity

Developing a robust security approach, that boosts integrity and public confidence in the electoral process can be enhanced by employing additional supporting tools, such as stakeholder outreach and development of collaborative efforts improve voting and election processes. The GMVS model addresses dimensions of certainty (assurance of security) and implementation (capacities, complexity of implementation cost) as a way of navigating the complexity of election security. Advantages of this approach include reduction of uncertainty due to the rapidly change technology and security landscape, cost savings to jurisdiction from simplified (and more assured) procurement specification, assessment and evaluation, and to vendors from having to repeatedly conduct security audits which may differ minimally from local to local, but which require redundant efforts to address. Overall, the ultimate benefit is to all stakeholders by potentially reducing one aspect of security uncertainty, while at the same time achieving cost-savings and increased public perception of election system integrity.

This research was sponsored by Smartmatic.

References

CSIS. (2018). *CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond.* Washington D.C.: Center for Strategic and International Studies. https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond (October 29, 2018)

Darnolf, S. (2018). Safeguarding Our Elections: Enhanced Electoral Integrity Planning. *SAIS Review of International Affairs*, *38*(1), 39-51.

Dunn, M., & Merkle, L. (2018, March). Overview of Software Security Issues in Direct-Recording Electronic Voting Machines. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 182).

GAO. (2018). Elections: Observations on Voting Equipment Use and Replacement. Washington D.C.: Government Accountability Office. GAO-18-294: Published: Apr 11, 2018. https://www.gao.gov/products/GAO-18-294

National Academies of Sciences, Engineering, and Medicine (NASEM). (2018). *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/25120.

University of Pennsylvania, Wharton School Public Policy Initiative. (2016). "The Business of Voting: Market Structure and Innovation in the Election Technology Industry." https://publicpolicy.wharton.upenn.edu/business-of-voting/