

Verified Voting Comments on Draft NISTIR 7682 - Information System Security Best Practices for UOCAVA-Supporting Systems

June 18, 2010

Given the current focus on UOCAVA implementation, the NIST draft Information System Security Best Practices for UOCAVA-Supporting Systems (referred to here as the Draft) is a timely and important document. A summary of security standards and guidelines "*deemed most applicable for jurisdictions using IT systems to support UOCAVA voting*" is indeed necessary at a time when many states are moving forward with Internet based voting, too often with insufficient thought to the security implications of casting votes online. The Draft acknowledges the urgency of proper security:

*"...security compromise could carry severe consequences for the integrity of the election, or the confidentiality of sensitive voter information. Failure to adequately address threats to these systems could prevent voters from casting ballots, expose individuals to identity fraud, or even compromise the results of an election."*¹

Unfortunately, the Draft falls short of providing the comprehensive analysis of security practices implied by the title. While the limitations and scope of topics are clearly laid out, the remaining gaps, particularly those related to online return of voted ballots, are too large and too important to ignore. Even with disclaimers, the Draft may encourage many in the target audience, the election officials and IT staff implementing UOCAVA voting², to believe that the controls outlined in the Draft are adequate to address all types of online voting, including return of voted ballots via Email.

Limitations of the Draft

The Draft provides a high level view of security controls, focusing on technical, operational, and assurance controls as well as voting system network and host protection. The Introduction states, "*this document provides a set of minimum security controls that should be applicable to any type of IT system used to support UOCAVA voting, including best practices for technical, physical personnel and procedural security of such systems.*"³ Other limitations noted in the Introduction confirm that the draft is less than comprehensive regarding the full range of potential UOCAVA deployments [*emphasis added*]:

*"The best practices in this document are intended to be broadly applicable to all voting systems supporting UOCAVA that leverage IT systems, but they do not cover all requirements for all UOCAVA voting systems. The baseline best practices provided must be augmented with additional safeguards depending on a jurisdiction's particular circumstances. After implementing the best practices described in this document, jurisdictions should carefully consider the type of UOCAVA voting system deployed, and its context of use to determine what additional security measures are required. **It may not be possible to protect system-specific threats, such as those that would be unique to ballot delivery or return systems, using only the best practices described in this document.***

*As described in NISTIR 7551 A Threat Analysis on UOCAVA Voting Systems, **some types of UOCAVA voting systems face threats that are very difficult to mitigate with current technology, such as remote voting from personal computers.** Jurisdictions must consider the potential threats to a UOCAVA voting system, along with the totality of security controls and measures implemented in the system, when determining whether the system is within an acceptable level of risk."*⁴

The Draft correctly notes that many systems incorporating Internet ballot return are impossible to secure. But this important limitation is given little attention anywhere else in the draft. Prominent disclaimers about the Drafts limitations, particularly regarding online ballot return, should be included rather than the brief mention in the current version.

¹ Draft NISTIR 7682, Executive Summary, page 1

² Draft NISTIR 7682, Executive Summary, page 2 - "The guidance in this publication will assist election officials in collaborating with system designers and administrators to define roles and establish processes that ensure the ongoing secure operation of the systems."

³ Draft NISTIR 7682, Section 1, Introduction, page 3

⁴ Draft NISTIR 7682, Section 1.1, Purpose and Scope, page 3

Inconsistent message on adequacy for all systems

While acknowledging limitations, the Draft often implies that recommended practices are adequate for all types of online voting. An example occurs in the Introduction ⁵ :

"Since there are many potential ways to use IT systems to support UOCAVA voting, it is infeasible to provide detailed best practices for every possible architecture application, and configuration. Instead, this document provides a set of minimum security controls that should be applicable to any type of IT system used to support UOCAVA voting, including best practices for technical, physical personnel and procedural security of such systems."

Here, the Draft notes the inability to cover all possible systems, but follows with the statement that the proscribed controls are *"applicable to any type of IT system used to support UOCAVA voting"*. Indeed, there is nothing incorrect about the declaration - the Draft does indeed provide general advice while glossing over details. But what will a typical election official considering an Email based voting system take away from this statement? In many cases, it may be the latter half, that the Draft provides them with *"...security controls that should be applicable to any type of IT system."*

The Draft continues in this vein in reference to online return of voted ballots. A list of UOCAVA supported activities covered by the Draft includes *"Remote electronic voting from personally-owned systems."* ⁶, but later this exclusion is briefly noted - *"the security of voters' personal computers is not addressed in this document."* Then, just a paragraph later we read that *"most of the best practices described in this document will be applicable to any internet-connected system that is important to the election process."* ⁷ Again, a confusing message for non-technical election officials, and for IT staff implementing UOCAVA voting.

An Example - Email Ballot Return

As an example, compare the list of technical security controls ⁸ with one voting technology being piloted by in some states - return of voted ballots via Email. The Draft lists eight high level categories of control - Identification and Authentication; Personally Identifiable Information Protection; Confidentiality; Integrity; Availability; Cryptographic Security; Communication Systems. But in the case of email ballot return, adequate security cannot be achieved in any one of these categories simply because many of the systems storing and forwarding an email are not under the control of election officials. Given the current interest in Email ballot return, the Draft must do more to make the target audience aware when its recommended controls are inadequate to protect such systems.

Possibly Prohibitive Cost of Recommended Controls

The Draft provides security recommendations, not a cost analysis. Mention of the expense of implementing the recommended controls is only peripheral, such as this note in the Identification and Authentication Controls Section:

"The security criticality of the various functions should be weighed against the cost inherent in and assurance provided by the available I&A options." ⁹

But securing remote voting to any reasonable degree is an extremely expensive and labor intensive effort beyond the reach of most counties. As an example, consider Section 6.8.1, Penetration Testing. The Draft calls for an important recurring test shortly before the election, which most county election offices would find hard to finance or execute in the hectic days prior to an election:

"The voting system should undergo penetration testing after it is fully deployed to ensure that the vulnerability assessment is conducted against the exact configuration that will be used to conduct the election. This testing should take place as near to the start date of the election as is feasible, to enable the penetration testers to take advantage of the most recent known vulnerabilities, while at the same time providing system owners, administrators and vendors an opportunity to mitigate any discovered vulnerabilities. The testing should be conducted by experienced experts in penetration testing." ¹⁰

⁵ Draft NISTIR 7682, Section 1, Introduction, page 3

⁶ Draft NISTIR 7682, Section 2, General Overview, page 5

⁷ Draft NISTIR 7682, Section 2.1, Overseas Voting Systems Components, page 6

⁸ Draft NISTIR 7682, Section 2.2, Technical Controls, page 6

⁹ Draft NISTIR 7682, Section 3.1.5, Best Practices for Voting Systems, page 16

¹⁰ Draft NISTIR 7682, Section 6.8.1, Penetration Testing, page 54

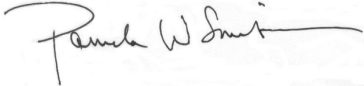
The necessary security measures for a UOCAVA system include facility and server hardening; additional staff; cryptographic and Virtual Private Network¹¹ implementations; penetration testing and much more. For local election officials facing already serious budgetary challenges, the cost of implementing the necessary security may be simply prohibitive.

Recommendations

The Draft is technically correct in acknowledging its limitations of scope. However, it is done in such a way that in combination with statements implying comprehensive treatment many in the target audience may reach incorrect conclusions about the Draft's applicability to systems they are investigating. We therefore recommend the following:

- Limitations should be clearly called out in a separate section.
- Statements that recommended procedures are applicable to all systems should be modified to note either specific or general exclusions.
- A section should be included noting specific forms of online voting which cannot be secured using proscribed controls such as email return of cast ballots.

Respectfully,



Pamela W. Smith
President, Verified Voting

¹¹ Draft NISTIR 7682, Section 4.3, Virtual Private Network (VPN) page 41 - "*The organization wishes to secure communication between two sites without going through the cost and inconvenience of providing cryptographic capability for each user and/or machine.*"