

# VVSG Cybersecurity Working Group

Update to the TGDC February 13, 2017

Joshua M Franklin



#### Overview

- Present Cybersecurity Principles & Guidelines
- Other Takeaways from the Working Group
- Discuss the Status of Previous Work Items
  - Need for Scope Determinations
  - VVSG 1.1 Gap Analysis



## Working Group Composition

- 100+ individuals on the mailing list, ~25 on the calls
- Primarily academics, scientists, engineers
  - Including previous TGDC appointees
- ~ 5 election officials actively participated
- ~ 5 technical manufacturer staff
- Election integrity advocates
- NIST and EAC staff



## Cybersecurity Principles

**Auditability** 

Ballot Secrecy Access Control

Physical Security

Data Protection

Software Integrity

Detection & Monitoring



## Auditability

## The voting system is auditable and enables evidence-based elections.

- An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results.
- The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities.
- Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.
- The voting system supports efficient audits.



## **Ballot Secrecy**

The voting system protects the secrecy of voters' ballot selections.

- Ballot secrecy is maintained throughout the voting process.
- Records produced by the voting system do not reveal how a voter voted.



#### **Access Control**

The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.

- The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.
- The voting system supports authentication mechanisms and allows administrators to configure them.
- Default access control policies enforce the principles of least privilege.



## **Physical Security**

The voting system prevents or detects attempts to tamper with voting system hardware.

- Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.
- Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing.



#### **Data Protection**

The voting system protects sensitive data from unauthorized access, modification, or deletion.

- Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.
- The source and integrity of electronic tabulation reports are verifiable.
- All cryptographic algorithms are public, well-vetted, and standardized.
- Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks.



## Software Integrity

Voting systems prevent the unauthorized installation or modification of firmware, software, and critical configuration files.

- Only software that is digitally signed by the appropriate authorities is installed on the voting system.
- The authenticity and integrity of software updates are verified by the voting system prior to installation and authorized by an administrator.



## Detection & Monitoring

The voting system provides mechanisms to detect and remediate anomalous or malicious behavior.

- Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.
- The voting system generates, stores, and reports to the user or election official, all error messages as they occur.
- Voting systems employ mechanisms to protect against malware.
- If the voting system contains networking capabilities, it employs appropriate modern defenses against networkbased attacks.



## Other Takeaways

- Possible principles not included:
  - Vulnerability Management
  - Software Freshness
  - Software Transparency
  - Timeliness of Software Updates
  - Risk Management
- Significant discussion on the degree of auditability, and how best to achieve it



#### Status of Previous Work Items

- Focus on areas clearly in scope as a starting point.
  - Complete
- General security recommendations for ballot delivery and marking (not return), BoD, results reporting, and auditing.
  - Ongoing
- Begin conversations between cyber/HF/testing regarding auditable systems and accessibility.
  - Not started
- Discussions on risks and benefits on electronic return.
  - Not started
- Scope and Gap Analysis status listed on the next slides



### Scope Determination

- The following items affect the scope of the VVSG:
  - Remote blank ballot delivery and ballot marking
  - The use of wireless (inside & outside the polling place)
  - Electronic pollbooks (activation and/or synchronization)
  - Voter registration systems
  - Ballot printing at polling places
- Need determinations <u>before requirements can be</u> <u>written</u>.



## VVSG 1.1 Gap Analysis

- This has not been a main area of focus for the group.
  - Likely the next task in the queue.
- Members of the VVSG Cybersecurity WG provided input.
- NIST and EAC staff met with 5 voting system manufacturers and voting system test labs.
- NIST is performing a full analysis of the relevant sections.



## A <u>special thanks</u> to the VVSG Cybersecurity Working Group members for their contributions of time and expertise.