NIST's Role in Election Security

ISPAB, December 2019

Gema Howell
Applied Cybersecurity Division, NIST
Gema@nist.gov

Agenda

- Introduction
- NIST's role
- VVSG basics, structure, process
- VVSG 2.0 development
- VVSG 2.0 cybersecurity requirements
- Interagency collaboration/cybersecurity framework profile
- Questions

Who am I?

- Computer Scientist / IT Security Engineer
- 5years working in voting at NIST
- NIST Lead for the cybersecurity efforts to develop the standards for the VVSG
  - Co-chair the Cybersecurity Public Working Group
- Volunteer as a poll worker in Baltimore City, MD

- Also focus on mobile device and wearable security
  - For deployment in the general enterprise
  - For specific application to Public Safety/First Responders

2016 General Election Attacks

- Data exfiltration from voter registration systems
- Phishing election officials & voting system vendors
- Doxing of political campaigns
- Attacks on backend, non-tabulation systems

"We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes." – *Office of the Director of National Intelligence*

An Expanding Threat Model

Traditional Attacks

- Physically proximate
- Accidental events
- Natural disasters
- Events affecting public confidence and trust

Recent Attacks

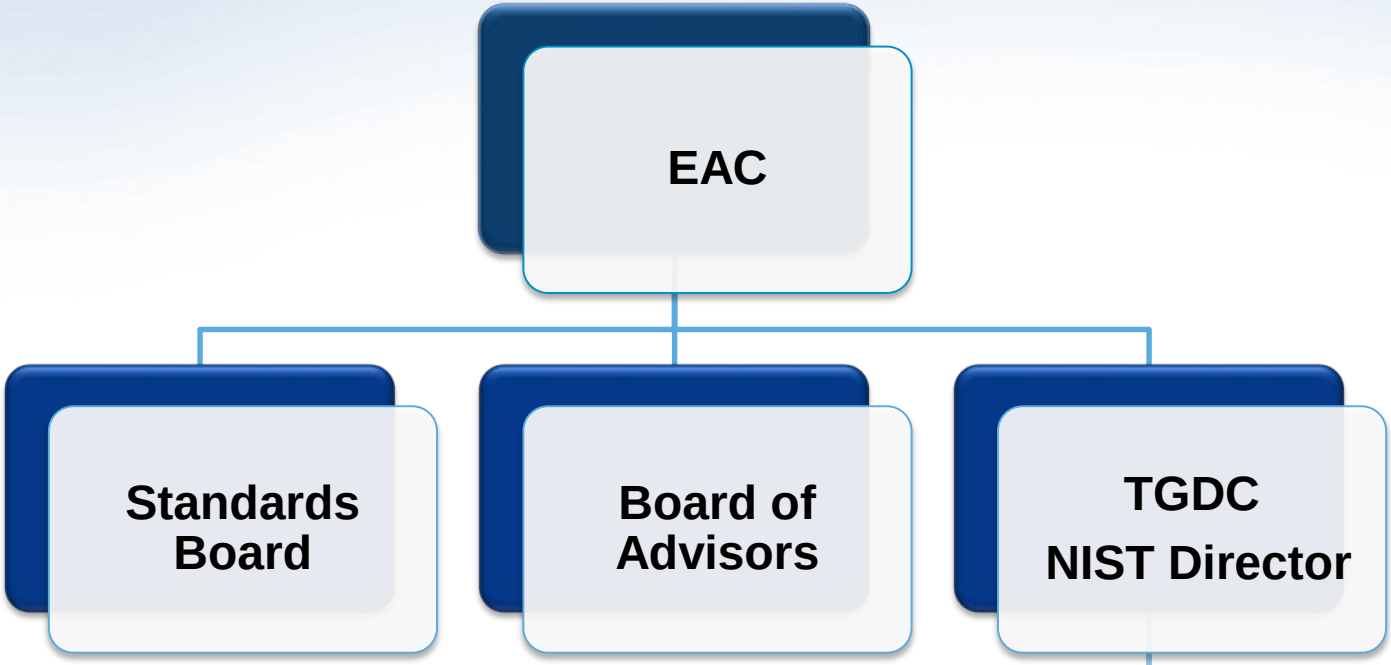
- Nation-state
- Phishing
- Attacks on supporting election systems
- Misinformation

NIST's Role in Voting

- Mandated by the Help America Vote Act of 2002
  - Technical Support to the U.S. Election Assistance Commission
- Standards & guidelines development
  - **Voluntary Voting System Guidelines (VVSG)**
  - Interoperability
- Research & assessment
  - Human factors
  - Cybersecurity
- Testing methodologies
- Test laboratories go through the National Voluntary Laboratory Accreditation Program (NVLAP)
- Best Practices
- **Interagency Collaboration/Cybersecurity Framework profile development for Election Infrastructure**

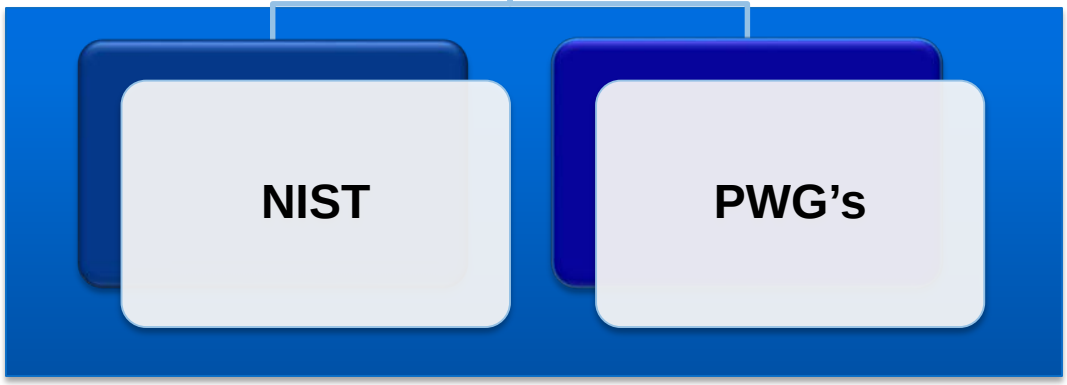
VVSG BACKGROUND

VVSG 2.0 Development



Voting Guidelines

- Tap into as many experts as possible
- Get continual feedback



NIST-EAC Public Working Groups

Election Groups

- Developed election process models that served as the basis for use cases and the core functions
  - Pre-Election (116 members)
  - Election: (98 members)
  - Post-Election: (78 members)

Constituency Groups

- Conducted gap analyses and developed draft VVSG 2.0 Principles and Guidelines, Requirements
  - U&A (123 members)
  - Cybersecurity (175 members)
  - Interoperability (182 members)
    - Election Modeling (45 members), Cast Vote Records (45 members)
    - Online Voter Registration (54 members), Voting Methods (46 members)
  - Testing (84 members)

Local and Online Voter Registration

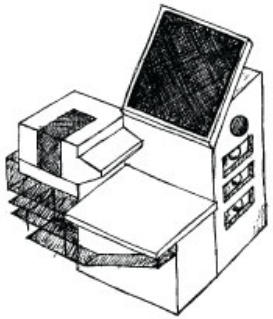
Electronic Pollbooks

Candidate Filing Systems

Campaign Voter Info Databases

Direct Record Electronic

Optical Scan



Ballot Marking Device

New Structure

For all stakeholders, plain language

Principles:
- High-level design goals

Guidelines:
- Broad system design details for election officials

Requirements:
- Low-level guidance for manufacturers and test laboratories

Test Methods:
- Guidance to ensure necessary breadth and depth when testing voting systems

VVSG 2.0: Principles and Guidelines

	Principles	Guidelines
General	15	52
Interoperability	3	10
Human Factors	5	12
Security	7	21
	18	**53**

- ***Feedback from NASED, SB, BoA***
- ***Discussed within/between PWGs***
- ***Simplified text, removed duplicates, merged categories***

15 Principles, 52 Guidelines

- *Principles*: High-level design goals
- *Guidelines*: Broad system design details for election officials
- Written in plain English
- *Requirements*: Low-level guidance for manufacturers/laboratories
- *Test Methods*: Guidance to ensure necessary breadth/depth when testing voting systems

- Engaged NASED, Standeards Board, Board of Advisors members in discussions and garner feedback
- Presented and adopted at TGDC September 2017 meeting

VVSG 2.0: Principles & Guidelines

	Principle	Guidelines
1	High Quality Design	3
2	High Quality Implementation	7
3	Transparency	3
4	Interoperability	4
5	Equivalent and Consistent Voter Access	2
6	Voter Privacy	2
7	Marked, Verified, and Cast as Intended	3

	Principle	Guidelines
8	Robust, Safe, Usable, and Accessible	3
9	Auditability	4
10	Ballot Secrecy	2
11	Access Control	5
12	Physical Security	2
13	Data Protection	4
14	System Integrity	4
15	Detection and Monitoring	4

Cybersecurity Requirements

Where to find the Security Requirements?

- The security requirements fall under Principles 9 through 15
- A few requirements that cover software security are under Principle 2
- Some areas of overlap with other principles

	Principle
9	Auditable
10	Ballot Secrecy
11	Access Control
12	Physical Security
13	Data Protection
14	System Integrity
15	Detection and Monitoring

	Principle
2	High Quality Implementation

How did we get here?

- Used 2007 VVSG Recommendations and VVSG 1.1 as baselines
- Updated based on feedback from VVSG Cybersecurity PWGs
- Updated based on review of new security innovations:
  - **Industry**
    - Secure boot and strong process isolation
    - Exploit mitigation technologies (e.g., ASLR, DEP)
    - Stronger network protocols
    - Security frameworks
  - **Voting Systems**
    - Software Independence
    - Risk Limiting Audits
    - E2E verifiable cryptographic protocols
    - Recognition of usability as a security issue

Principle 9 – Auditable Overview

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

- 4 Guidelines
- Focuses on machine support for post-election audits
- Software independence mandatory
- Support for paper-based and end-to-end verifiable system
- Support for risk-limiting audits (RLAs)

Principle 10 – Ballot Secrecy Overview

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

- 2 Guidelines
- New section that distinguishes ballot secrecy from voter privacy
- Prevents association of a voter identity to ballot selections

Principle 11 – Access Control Overview

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

- 5 Guidelines
- Significant updates made to strengthen monitoring of access and ensure critical operations are performed by authorized users
- Require multi-factor authentication for critical operations

Principle 12 – Physical Security Overview

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

- 2 Guidelines
- Mostly unchanged
- Exposed physical ports must be essential to voting operations
- Physical port must be able to be logically disabled
- All new connections and disconnections are logged

Principle 13 – Data Protection Overview

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

- 4 Guidelines
- Protection of election artifacts
- No hardware security requirements (e.g., TPM)
- Require FIPS 140-2 validated cryptographic modules

Principle 14 – System Integrity Overview

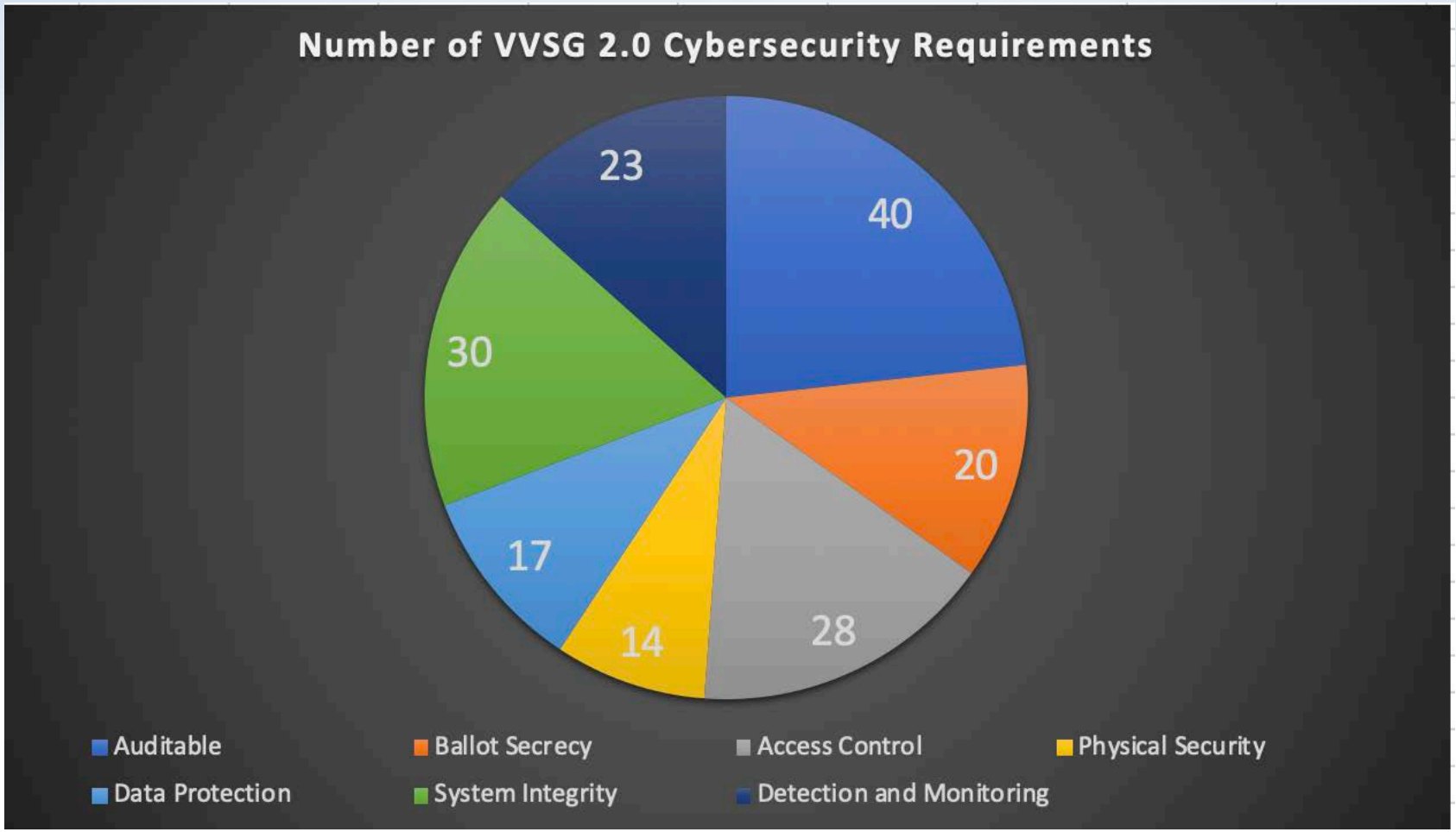
The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

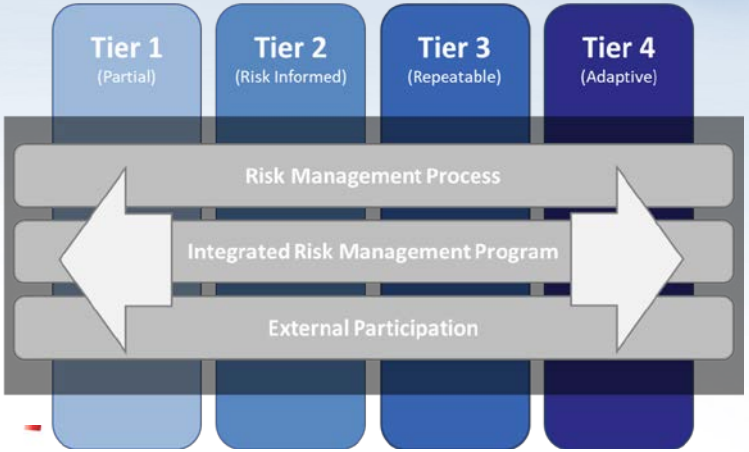
- 4 Guidelines
- New section of the VVSG to include strategies and techniques to protect the voting system as a whole
- Require risk assessment and supply chain risk management strategy
- Secure configurations and system hardening
- Exploit mitigation (e.g., ASLR, DEP) and free of known vulnerabilities
- Cryptographic boot validation
- Authenticated updates
- Sandboxing and runtime integrity

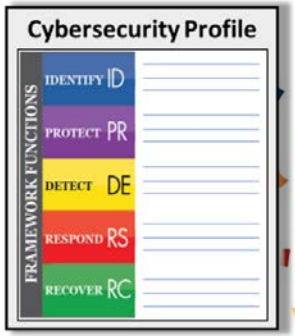
Principle 15 – Detection and Monitoring Overview

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

- 4 Guidelines
- 23 Requirements
- Moderately updated list of log types
- Firewalls & IDS for networked systems
- Must be updateable
- Digital Signatures / whitelisting for voting systems
- Malware detection focusing on backend PCs
- Does not include DREs, Opscans, or BMDs


Number of VVSG 2.0 Cybersecurity Requirements
40
20
28
14
17
30
23
Auditable
Ballot Secrecy
Access Control
Physical Security
Data Protection
System Integrity
Detection and Monitoring





NIST Cybersecurity Framework

Election Infrastructure Profile

Using the Cybersecurity Framework

- Developing a baseline profile to cover the election infrastructure
- Highlight high priority security expectations
- Point to related informative references
- Allow for self assessment comparison
- Provide an example profile for others to develop their own
- Work with the DHS's Election Infrastructure Sub-sector Working Group that consists of the GCC and SCC

Questions?