VVSG 2.0 Update

Standards Board, April 2019

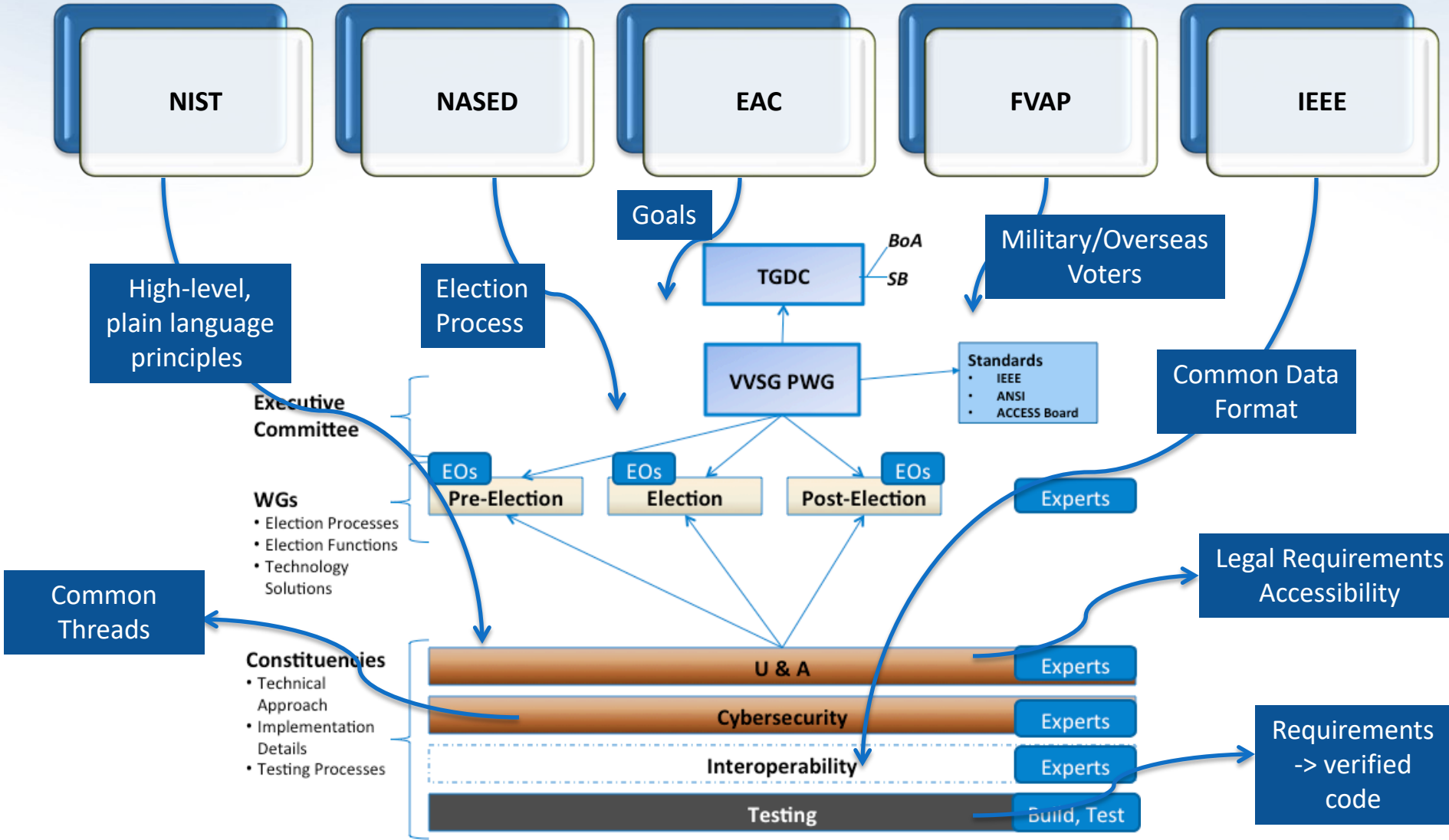
Mary Brady
Mbrady@nist.gov

Sharon Laskowski
Sharon.laskowski@nist.gov

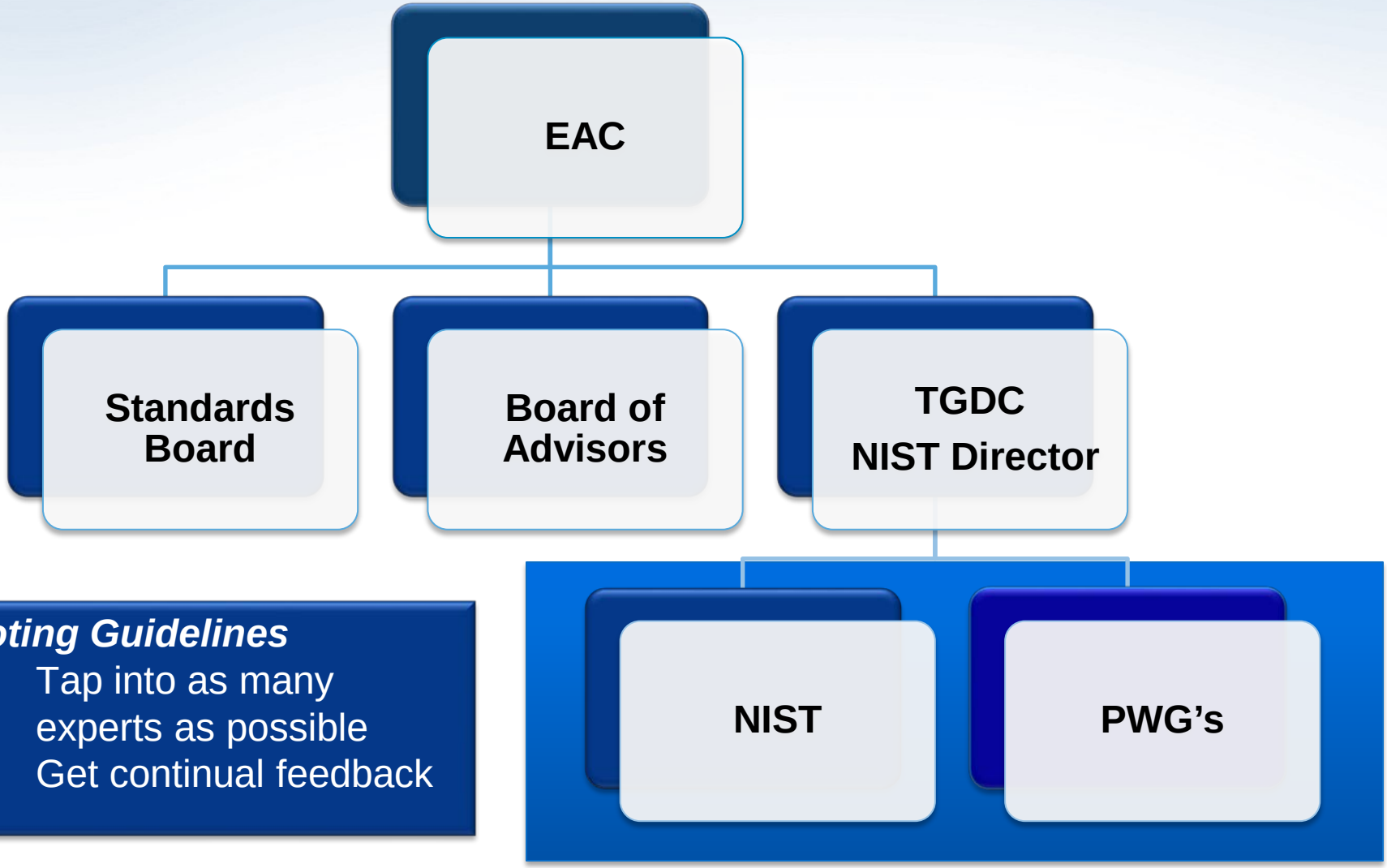
Gema Howell
Gema.Howell@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

Together…Making It Happen



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)

Reaching Consensus on VVSG Scope

Election WGs

Pre, Election, and Post

Election Process Models

- TGDC
- EAC/NIST
- PWG Chairs

Use Case Scenarios

Core Functions

- Standards Board
- Board of Advisors
- NASED

A New VVSG Structure

HIGH LEVEL
Principles

LOW LEVEL
Test Assertions

- NASED Subgroup / NIST
- EAC VVSG Futures Group
- NASED Input to EAC / NIST
- EAC Roundtable / Public Meetings
- TGDC, SB, BoA Adoption

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
- Greatly reduced size: ~~**221,38, 20, 10**~~**,5 pages!**
- *Requirements*: Low-level guidance for manufacturers/laboratories
- *Test Methods*: Guidance to ensure necessary breadth/depth when testing voting systems

- Engaged NASED, SB, BoA 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

Open Issues

Area	Topic	Use cases	Concerns
Cybersecurity	Network Connectivity – wireless, bluetooth, cellular networks	Print ballots from a ballot marking device, attach accessibility devices, transfer results.	• Modification of voter choices, results • Eavesdropping • Injection of malware
	E2E Cryptographic Systems	An alternative software independent option to paper-based systems; allows for innovation	• Few examples of existing E2E systems • Potentially confusing to understand
	Barcode encoding schemes	Ballot activitation, apply usability configs, store ballot selections, transfer tabulation results, pre-voting, store identifiers, store digital signatures	• Lack of Transparency • Violation of Ballot Secrecy • Interoperability • Auditability • Misinformation used for tabulation
	Indirect ID	Associate an individual with a provisional ballot until the voter can be validated	• Violation of Ballot Secrecy Principle

Open Issues

Area	Topic	Use Case	Cons
Human Factors	Ballot submission with little or no use of hands	Allows voter to vote privately and independently	Increased cost to manufacture
	Vote Selection Only Ballots	Simple ballots may help many voters – low literacy, low dexterity, etc.	Not voter-verifiable
Interoperability	Required Common Data Formats	Election Officials support - improves auditability, transparency and interoperability – will allow for plug-and-play interoperability	• CDFs aren't yet in widespread use • Not a sufficient need • Who addresses problem if voting system is hybrid?

Requirements

General Working Guidelines

- Used VVSG's 1.1, 2007, and updated research as baselines
- Updates based on feedback from VVSG PWGs, interactions with manufacturers and labs
- Recent discussions on where requirements belong – inside the VVSG, an external document, or with the EAC

Design, Implementation

Principle	Technical Areas	What's New?	Status
P1	1.1 Specification of voting processes, functions, and logic 1.2 Their accuracy and limitations (logical and volume limits) 1.3 Their testability	• EO Tests: Examine CVR, audit barcodes against human-readable paper. • Insert ID into CVR for 1-1 mapping btwn ballot and CVR. • ID can be pre-printed, barcode on scan or by BMD. • EMC Updates, external pointer	• Draft requirements for all sections • Sync'ed with core functions • VVSG Requirements / EAC policy and procedures
P2	Implementing systems using best-practices in HW, SW, telecom, data, QA/CM, human factors, security, and interoperability. 2.1 – Use of trustworthy materials and SW best practices 2.2 – User-centered design best practices 2.3 – Design/Implementation of system logic (HW, SW, …) 2.4 – Design/Implementation of system architecture. 2.5 – Preserving integrity across the system's layers. 2.6 – Error handling and recovery. 2.7 – Reliability and accuracy in physical environment.	• Met with EAC to discuss where most of this belongs? • Requirements point to external documentations that will provide evolving best practices	• Draft requirements complete • Need additional external guidance, based on internal discussions btwn NIST/EAC.

Considerations for Existing Requirements

- **Existing requirements tend to overlap with other standards or may better be located elsewhere, including for:**
  - Software quality and workmanship
  - Programming languages and coding standards
  - Hardware and electrical testing
  - Temperature and humidity
  - Testing techniques
  - Documentation (TDP, test plan)
- **Under consideration:**
  - Remove overlapping requirements and point to external standards as applicable
  - Relocate some requirements to external guidance or, possibly, the EAC certification manuals, e.g., testing techniques, documentation
- **Advantages include:**
  - A smaller, better focused VVSG
  - External standards offer more flexibility when it comes to updates

High Quality Design

- **Synopsis:**
  - 1.1 - Specification of voting processes, functions, and logic
  - 1.2 - Their accuracy, reliability, and limits (logical / volume limits)
  - 1.3 - Their testability.
- **Status:**
  - 1.1 draft requirements covering activities by voting activity, synchronizing Core Functions with benchmarks work
  - 1.2 draft requirements for accuracy, misfeed-rate, volume, stress, and reliability testing requirements and logical limits from VVSG 2007 – reviewing with statisticians, externalizing benchmark information, and updating for Core Functions
  - 1.3 have draft requirements for implementation statement, referring to Core Functions instead of classes, externalizing references to benchmarks and supporting information, externalizing documentation and testing information to EAC manuals

High Quality Implementation

- **Synopsis:**
  - This principle is about implementing systems using best-practices in HW, SW, telecom, data, QA/CM, human factors, security, and interoperability. They are about the following:
    - 2.1 – Use of trustworthy materials and SW best practices
    - 2.2 – User-centered design best practices
    - 2.3 – Design/Implementation of system logic (HW, SW, …)
    - 2.4 – Design/Implementation of system architecture.
    - 2.5 – Preserving integrity across the system's layers.
    - 2.6 – Error handling and recovery.
    - 2.7 – Reliability and accuracy in physical environment.
- **Status:**
  - 2.1, 2.3-2.6 – have draft requirements, externalizing detailed tech guidance for smooth evolution of tech
  - 2.7 – have draft benchmark requirements for environmental tests (humidity, temperature, shock, vibration); working with statisticians to finalize benchmarks and validate test references

Benchmark Requirements

- Benchmarks are for performance measures: reliability, accuracy, misfeed-rate, volume, stress, and environmental concerns
- Previous VVSGs included benchmarks, requirements, and tests in a single document
- New division of labor/content
  - NIST is in the process of publishing benchmark definitions externally, referring to them from VVSG/requirements
  - Discussions with the EAC on maintaining tests that refer to requirements and benchmarks from their manuals

Reliability Benchmark

Formerly (1.x)

- Reliability concept: more narrowly focused
- Single traditional measure (MTBF) for just equipment
- Not end-to-end
- Not really representative of reliability during operational life

VVSG 2.0

- Reliability concept: more broad, end-to-end
- Adjusts reliability measure to apply to all tests (end-to-end), including volume test
- Increased focus on use of high quality engineering to decrease chance of failures in testing/ops
- Volume test remains representative throughout equipment lifecycle
- Defined on critical and non-critical failures
- Working with statisticians on experimental design for coverage and testing costs

Accuracy Benchmark

1.x

- Focus: sequential testing, variable length
- Calculations based on Bernoulli probability calculations
- Not as representative of actual failure patterns

VVSG 2.0

- Focus: end-to-end
- Includes volume test derived from CA volume test
- Calculations based on Poisson probability calculations
- More representative of actual failure patterns
- Working with statisticians on experimental design for coverage and testing costs

Physical Environment

- Simulates physical influences on equipment during operational life: storage, transport, setup, operations
- Influences: Humidity, temperature, shock, vibration, mechanical, electrical, magnetic, and more
- Based on environmental benchmarks and tolerance levels
- In all cases, system's default before and after states are captured and it is asked to perform election tasks accurately even with shifts in humidity, temperature, etc.
- Most of these environmental tests, procedurally, are very similar
- Each one may require specialized setup/expertise to run and interpret
- Especially the effects of *temperature* and *power*, can be very significant for the physical stability of equipment operations, but also costly
- Working with statisticians on experimental design for coverage and testing costs

Volume/Stress

- Modeled after CA volume test
- Used with reliability and accuracy
- Based on mock election benchmarks, and estimated failure rates
- Simulates representative med-complexity county election
- Tests entire system
- Preserves accuracy
- Observes behavior up to and beyond published limits (max contests, max vote positions, etc.)
- Demonstrates operational logical and performance stability
- Working with statisticians on experimental design for coverage and testing costs

Transparency, Interoperability

Principle	Technical Areas	What's New?	Status
P3	• Voting system is high quality • Can be inspected, e.g., audits and checks available at various stages • Simple in structure	Include voting system documentation requirements, functional requirements for audits between operational stages, and for linking ballots to their cast vote records for correspondence audits Link requirements from interoperability (transparency of data), security (easier to audit).	• Complete
P4	• Common hardware/software interfaces • Common data formats for imports/exports • COTS devices in the voting system • Capability to integrate other-vendor devices into a voting system	Synchronized with CDFs COTs permitted as long as other requirements are met Imports/exports must include CDF support	Complete

Interoperability Requirements

- Hardware interfaces must be industry-standard
- COTs are permitted as long as other requirements are met
- Imports and exports must include common data format (CDF) support:
  - Election definition and results reporting
  - Event logging
  - Cast vote records
  - Voter records interchanges

Common data formats (CDF)

- Use in import and export of election data
- Aim is to improve usability of data for election officials and interoperability between devices
- Tie-ins to usability, security and transparency
- Four main areas:
  - Election event logging
  - Election programming and results reporting
  - Cast vote records
  - Voter registration-related transactions and data

Functional Requirements

- Deals with behavior of voting system during phases of running an election:
  - Election and Ballot Definition
  - Pre-election Setup and L&A Testing
  - Opening Polls, Casting Ballots
  - Closing Polls, Results Reporting
  - Tabulation, Audit
  - Storage

Functional Requirements

- Coordinated with cybersecurity in areas including
  - Pre-election setup
    - Audits of bar codes vs readable content for BMDs
    - Audits of scanned ballot images vs paper ballot
    - Audits of CVR creation
  - Contents of various reports
  - Audit
    - Ensure capability to match a ballot with its corresponding CVR

User Documentation

- Discussions with EAC on moving the test lab-related requirements that are currently included in VVSGs 1.0 and 1.1 to EAC test & cert manuals
- User documentation requirements from the TDP remain in the VVSG.
- User documentation deals with all aspects of operation, maintenance, and storage, with emphasis on security
- Also includes requirements for training documentation

CDF Open Issue

- Major manufacturers are generally supportive of CDFs but on-going discussions regarding how to implement:
  - CDFs aren't yet in widespread use, not a sufficient need
  - They contribute to component certification
  - If voting system is mixture of components from different manufacturers, who do you go to if something is wrong?
- Election officials and others in PWG support the CDFs being required in the next VVSG

Human Factors

Principle	Technical Areas	What's New?	Status
P5-P8	Usability & Accessibility	• Updated and less-prescriptive, based on >10 years of voting & usability research • Harmonized with current accessibility standards (Section 508, Web Content Accessibility Guidelines, etc. • Organized according to the widely-accepted accessibility POUR principles (Perceivable, Operable, Understandable, and Robust). • Addresses all modes of presentation (visual, audio, enhanced video) and interaction (touch, tactile, non-manual)	• Complete • Drafts of explanatory/ guidance documents

Human Factors Requirements

- Assumption: All electronic voter interfaces meet all applicable accessibility (and usability) requirements
  - VVSG 1.0, 1.1 made a distinction between accessible and non-accessible electronic voting systems based on the products and state of the art in 2005
- Updated and less-prescriptive
  - Based on >10 years of voting & human factors research
- Harmonized with current federal accessibility standards
  - Section 508, Web Content Accessibility Guidelines, etc.
- Organized according to the widely-accepted accessibility POUR principles
  - Perceivable, Operable, Understandable, and Robust
- Addresses all modes of interaction
  - Visual, enhanced visual, audio, tactile, non-manual, limited dexterity control

Status of Human Factors Requirements

- Completed draft requirements
  - Extensive discussions with the NIST Human Factors Public Working Group
  - Scope is Principles 5 through 8 and Principle 2 Guideline 2
- Completed drafts of explanatory/guidance documents for developers/designers, testers, and election officials
  - Ballot: Text size, color&contrast, select/deselect, scrolling&paging, review screen navigation
  - Assistive Technology in the polling place
  - User-centered design and usability testing
- Completed drafts of report templates (and guidance) for use by developers for user-centered design and usability testing with voters and poll workers

What's New in HF Requirements

- All modes of interaction and presentation applied throughout the voting session, fully supporting accessibility (P5)
- Distinguished voter privacy from ballot secrecy and ensured privacy for marking, verifying and casting the ballot (P6)
- Updated voter interface requirements such as font, text size, audio, interaction control and navigation, scrolling, ballot selections review (P7)
  - Voting system specific, but derived from Federal accessibility law

What's New in HF Requirements(2)

- Reference to Federal accessibility standards (P8)
  - Section 508, WCAG 2.0
- Updated requirements for reporting of developer usability testing with voters and election workers (P8)
- New requirement to document and report on user-centered design process by developer (P2.2)
  - To ensure system was designed for a wide range of representative voters, including those with and without disabilities, and election workers

Issues

- Casting a paper ballot privately and independently without manually handling the ballot
  - This VVSG requirement has been difficult to implement--must be able to verify the ballot selections and cast easily
  - Los Angeles County VSAP ballot marker is one solution
    - Ballot rolls out after marking for verification then rolls back into a ballot box
    - Can do central counting since there are no overvotes on an electronically marked ballot
- Designing electronic ballot markers so voters will and can easily verify the paper ballot/vote record
  - Older approaches were not usable, e.g., under glass, hard-to-read
  - We are now seeing more attention to information design

Next Steps for Human Factors

- Work with other PWGs to ensure accessibility and usability is supported in other parts of the VVSG 2.0
- Finalize VSSG 2.0 requirements and guidance
- Update test methods
- Two webinars planned for explaining the updated and new requirements
- Verification of ballot selections by voters
  - Research project underway to explore how to design the voting process for ballot marking systems to encourage voters to verify and to support accurate verification through good information design
- Other guidance as needed, e.g.,
  - Dual switch navigation guidance for limited dexterity control
  - Audio voicing and instructions

Status of Human Factors Test Methods

- Completed drafts of report templates and guidance for use by developers for user-centered design (P2.2) and usability testing with voters and poll workers (P8.3, P8.4)
- Completion of test methods and materials expected January 2020

Security

Principle	Technical Areas	What's New?	Status
P9-P15	Auditability Ballot Secrecy Access Control Physical Security Data Protection System Integrity Detection and Monitoring	Software independence, auditable records, voter info protection, unique ids for RLAs, multifactor auth for critical operations, requires 140-2, signing, encryption, new system integrity requirements, moderate updates on detection and monitoring	Largely complete, Some open issues

Overview

- Used 2007 VVSG Recommendations and VVSG 1.1 as baselines
- Updates based on feedback from VVSG Cybersecurity PWGs
- Updates 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

Status of Security Requirements

- Complete set of draft security requirements
  - Scoped to Principles 9 through 15
  - Discussed and reviewed by the NIST Cybersecurity Public Working Group
- Five open areas are currently under discussion:
  - Barcodes and Encoding Schemes
  - Wireless Technology
  - Internet Technology
  - E2E Systems
  - Indirect Voter Associations

What's New in the Security Requirements

- **Auditability Requirements**
  - Focuses on machine support for post-election audits
  - Software independence mandatory
  - Support for paper-based and E2E system
  - Support for risk-limiting audits (RLAs)
- **Ballot Secrecy Requirements**
  - Dedicated ballot secrecy section
  - Prevents association of a voter identity to ballot selections

What's New - Continued

- **Access Control Requirements**
  - Prevents the disabling of logging
  - Access control based on voting stage (Pre-voting, Activated, Post-voting)
  - RBAC not required
  - Require multi-factor authentication for critical operations:
    - Access to admin account
    - Software updates to the certified voting system
    - Aggregation and tabulation
    - Enabling network functions, wireless and use of telecommunications
    - Changing device states, including opening and closing the polls
    - Deleting the audit trail
    - Modifying authentication mechanisms

What's New - Continued

- **Physical Security Requirements (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
- **Data Protection Requirements**
  - No hardware security requirements (e.g., TPM)
  - Require FIPS 140-2 validated cryptographic modules
    - Except for E2E cryptographic functions
  - Cryptographic protection of various election artifacts
    - Digitally signed tabulation reports
  - Transmitted data is encrypted with end to end authentication

What's New - Continued

- **System Integrity Requirements (new area, significant update)**
  - Require risk assessment and supply chain risk management strategy
  - Remove non-essential services
  - 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
- **Detection and Monitoring 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

Open Areas in Cybersecurity Requirements

Indirect Voter Associations

Use Cases

- Conditional Ballots
  - Provisionals
  - Absentee/Military Voting
  - Change of Eligibility

Primary Concerns

- Violation of Ballot Secrecy Principle
  - If the indirect voter association can be used to link a voter to their ballot selections

Residual Risk

- If indirect voter associations are not allowed in voting systems…
  - Removing an ineligible voter's ballot must be process-based and handled externally from the certified voting system

Internet Connectivity

Use Cases

- Online Voting – UOCAVA
- Remote Access Software
- Transmit Election Results
  - Cellular Modems
  - Telephone lines (PSTN)

Primary Concerns

- Nation-state attacks
- Remote access of system
- Modification of vote totals
- Compromised Infrastructure (Malware)
- Denial of Service (DoS)

Residual Risk

- If Internet is banned then…
  - States may need to purchase new voting systems
  - There may be slower election result transmission
    - Especially for rural or mountainous areas.

Cryptographic End-to-End (E2E) Systems

Use Cases

- A software independent option that has an added security measure
- E2E systems can apply to paper and paperless systems.
- Allow voters to verify their ballot selections are correctly recorded and tabulated, without revealing their selections.
- Examples: Scantegrity, Scratch & Vote, Punchscan, Prêt à Voter (PaV)

Primary Concerns

- Few examples of existing E2E systems
  - Unclear if current requirements are sufficient
- Potentially confusing to understand
- Dispute resolution

Residual Risk

- If E2E systems are not included in the requirements…
  - Then it may limit the potential for innovation
  - It eliminates a system that can allow voters to verify their ballot is tabulated correctly

Wireless Technology

Use Cases

- Print ballot from printer (Wi-Fi)
- Activation Card or token for authentication (NFC)
- Transmit local/central tabulation results (Cellular)
- Assistive technology, peripheral devices (e.g., mouse, keyboard) - (Bluetooth)

Primary Concerns

- Modification of voter choices
- Modification of results
- Eavesdropping
- Injection of malware

Residual Risk

- If wireless is banned, then….
  - States may need to purchase new voting systems.
  - There may be slower transmission of election data
  - There may be longer lines due to a slowed voting process
  - There may be limited options for accessibility

Barcode and Encoding Schemes

Use Cases

- Ballot Activation
- Apply Usability Configurations
- Store Ballot Selections
- Transfer Tabulation Results
- Pre-voting
- Store Identifiers
- Store Digital Signatures

Primary Concerns

- Lack of Transparency
- Violation of Ballot Secrecy
- Interoperability
- Auditability
- Misinformation used for tabulation

Residual Risk

- If barcodes/encoding schemes are banned, then….
  - States may need to go through the acquisition and certification process for a new voting system
  - Voting systems may be less accessible to voters
  - There may be increased wait times at precincts
  - There may be increased time spent completing tabulation, audit, or recount

Next Steps for Cybersecurity

- Finish open area discussions to fully understand the use cases, concerns, mitigations and residual risk.
  - Add/remove/modify requirements based on TGDC feedback
- Review software security requirements that fall under Principle 2
- Develop list of test strategies that can be used for testing and certification of the security requirements.

Test Assertions

Test Assertions: Low-level details

Draft from VVSG

In-Depth Review

Feedback

- **Over 1200 TA's Developed for VVSG 1.0, 1.1**
- **Conducted Gap Analysis between VVSG 1.0, 1.1, and 2.0**
- **Explored test scenarios, rethinking strategy**

U&A: An Example

- **Principle:** No interference
- **VVSG 1.0 Requirement 3.2.2.2c-iii**: No voting equipment shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Devices and Hearing Aids, ANSI C63.19.
  - **TA3222ciii-1**: Voting equipment, when used with assistive hearing devices, SHALL achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.
  - **TA3222ciii-1-1**: Voting equipment, when used with cochlear implants, SHALL achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.
  - **TA3222ciii-1-2**: Voting equipment, when used with hearing aids, SHALL achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

Current Status

- Additional testing efforts:
  - Overall
    - Conducted Gap Analysis
    - Explored Scenario test generation
  - Human Factors
    - Completed drafts of report templates and guidance for use by developers for user-centered design (P2.2) and usability testing with voters and poll workers (P8.3, P8.4)
  - Cybersecurity
    - Discussing test method strategies

Questions