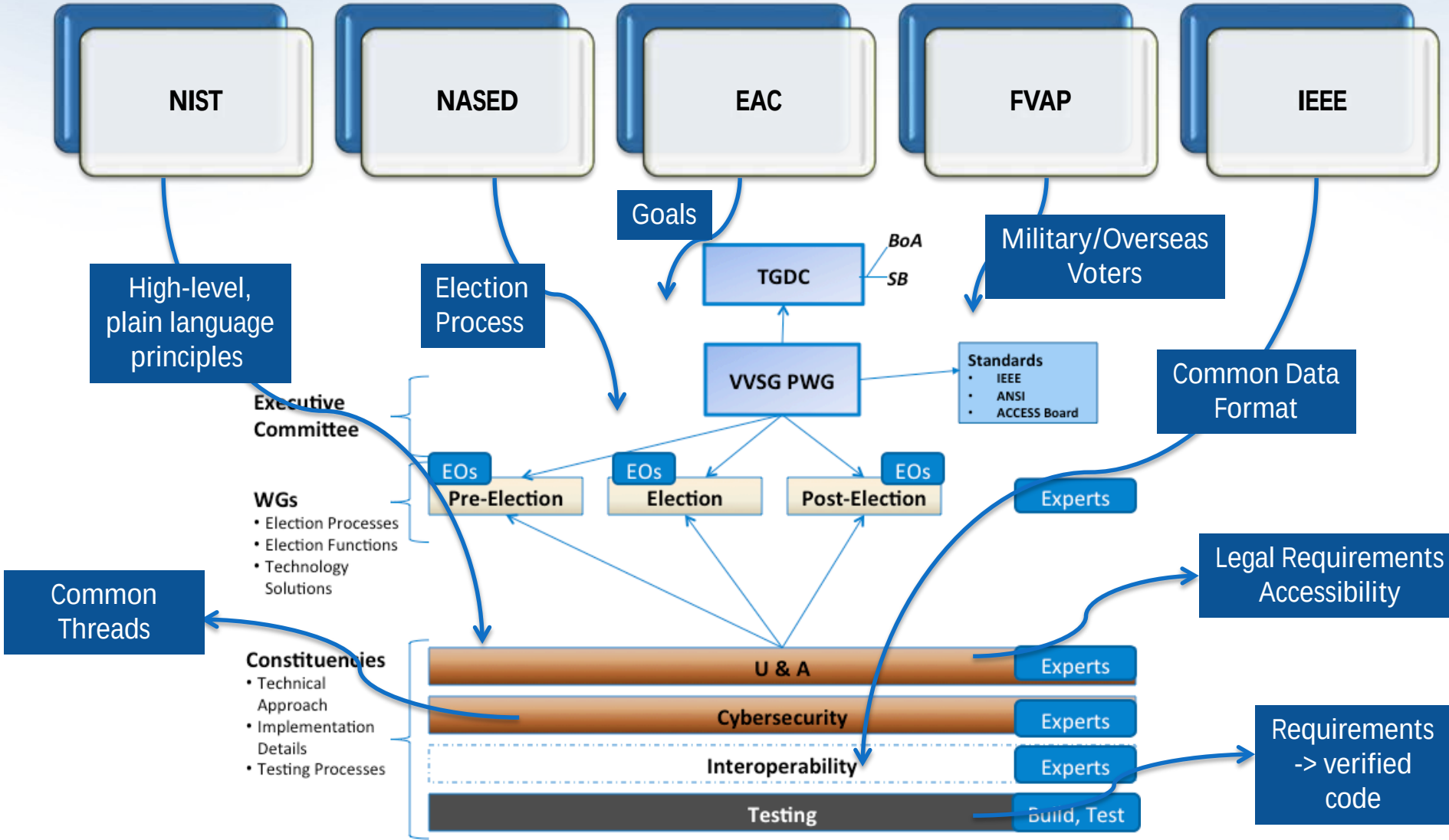
VVSG 2.0 Update

TGDC Meeting

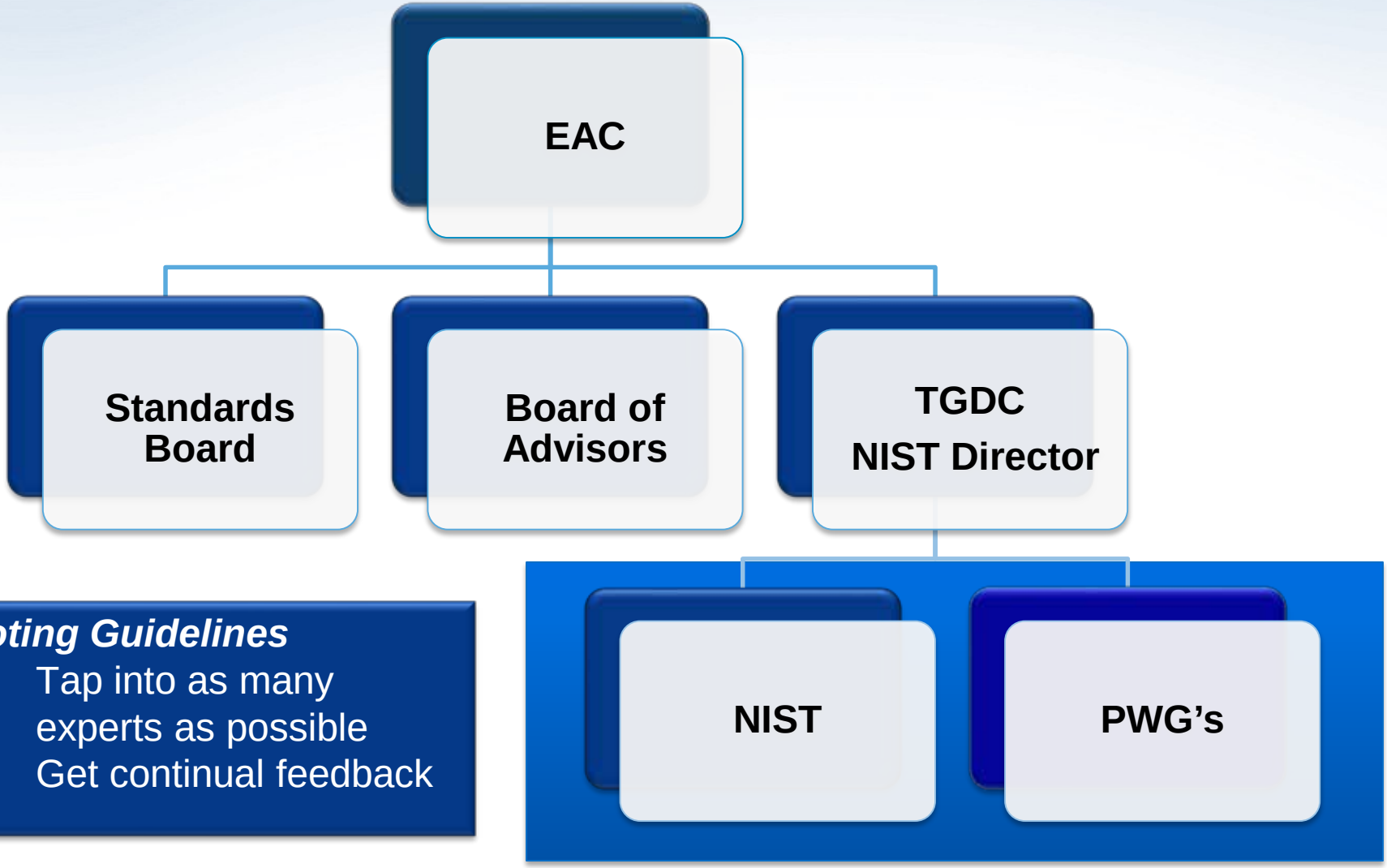
Mary Brady, NIST
Mbrady@nist.gov
April 2019

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

Together…Making It Happen



VVSG 2.0 Development



Voting Guidelines

- Ø Tap into as many experts as possible
- Ø 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 (103 members)
  - Election: (107 members)
  - Post-Election: (96 members)

Constituency Groups

- Conducted gap analyses and developed draft VVSG 2.0 Principles and Guidelines
  - U&A (105 members)
  - Cybersecurity (121 members)
  - Interoperability (158 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

Requirements

General Working Guidelines

- Used VVSG's 1.1, 2007, and updated research as baselines
- Updates based on feedback from VVSG PWGs, interactions with vendors 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 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

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

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

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

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

System Integrity Requirements

- **New area, significant update**
- Risk assessments mandatory
- Removal of non-essential services
- Secure configurations and system hardening
- Use of exploit mitigation tech (e.g., ASLR, DEP)
- Free of known vulnerabilities
- Cryptographic boot validation
- Sandboxing and runtime integrity
- Authenticated updates

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	Used to 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 • They contribute to component certification • If voting system is mixture of components from different manufacturers, who to blame if problems

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