OCT 1 3 2017

Mr. Brian Newby
Executive Director
U.S. Election Assistance Commission
Silver Spring, MD 20910

Dear Executive Director Newby:

In my capacity as the Chair of the Technical Guidelines Development Committee (TGDC), and as set forth in Section 221 of the Help America Vote Act (HAVA), I am pleased to advise you that the TGDC voted to recommend the attached version of the Voluntary Voting System Guidelines (VVSG) Principles and Guidelines to the Election Assistance Commission. Pursuant to Section 222 of HAVA, in developing the voluntary voting system guidelines and modifications of such guidelines, the Executive Director of the Commission shall take into consideration the recommendations provided by the TGDC. As adopted by the TGDC on September 12, 2017, please accept the attached version of the VVSG Principle and Guidelines, as the version recommended by the TGDC.

Sincerely,

Kent Rochford
Chair, Technical Guidelines Development Committee
Acting Under Secretary of Commerce for Standards and Technology &
Acting Director, National Institute of Standards and Technology

3

NIST

1. Voluntary Voting System Guidelines (VVSG) 2.0 Background

The United States Congress passed the Help America Vote Act of 2002 (HAVA) to modernize the administration of federal elections, marking the first time in our nation's history that the federal government has funded an election reform effort. HAVA provided federal funding to help the states meet the law's uniform and non-discretionary administrative requirements, which included the following new programs and procedures: 1) provisional voting, 2) voting information, 3) statewide voter registration lists and identification requirements for first-time registrants, 4) administrative complaint procedures, and 5) updated and upgraded voting equipment.

HAVA also established the U.S. Election Assistance Commission (EAC) to administer the federal funding and to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. Section 202 directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software. The purpose of the guidelines is to provide a set of specifications against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems.

This document, the *Voluntary Voting System Guidelines version 2.0* (*VVSG 2.0*), is the fifth iteration of national level voting system standards that has been developed. The Federal Election Commission published the first two sets of federal standards in 1990 and 2002. The EAC then adopted Version 1.0 of the VVSG on December 13, 2005. In an effort to update and improve version 1.0 of the VVSG, on March 31, 2015, the commissioners unanimously approved VVSG 1.1. Version 1.1 provided updates to requirements in the areas of security, reliability, usability, and accessibility. These improvements enhance the testability and clarity of some of the requirements contained in version 1.0 of the VVSG.

2. VVSG 2.0 Structure and Scope

In 2015, the Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) embarked on a new process that has been utilized in other industries by creating a series of public working groups to inform the development of the VVSG 2.0. The goal of the new process was to accelerate the development and adoption of the VVSG 2.0 by leading these working groups in close consultation with election officials, the federal and private sectors, developers, standards organizations, EAC committees, academic researchers, and other members of the public. The EAC and NIST areas of focus for the working groups are in voting system technology, including interoperability, human factors/accessibility, security, and testing.

To fulfill the Objectives of VVSG 2.0 as described in the Project Charter of the Technical Guidelines Development Committee (TGDC), the TGDC moved to adopt the scope and structure contained within this document. Moving forward, VVSG 2.0 and future iterations of this document will eliminate the previous focus on specific voting devices and components.

Instead, it will focus on the functions that those devices and components perform.

2.1. Structure

The VVSG 2.0 differs significantly from previous versions of the VVSG because it consists of high level principles and guidelines. The Principles are high-level system design goals. The Guidelines are broad statements of goals that meet the principles. This new structure has significantly decreased the size and complexity of the VVSG from previous versions making it easier to understand by the election community and other interested parties.

The standard is organized according to a logical structure intended to facilitate these aims on behalf of a diverse set of stakeholders who will need to use this information at varying levels of detail to achieve various tasks. The structure of the standard organizes and states the logical properties of voting systems in a hierarchical manner allowing communication of the most high-level information at the level of the principles and guidelines and more detailed refinements of that information at the level of requirements and test assertions. By separating the two documents, the Guidelines may remain constant while allowing the requirements and test assertions to be adaptable to constantly evolving technology.

The VVSG Version 2.0 will also have accompanying documents that detail requirements for how systems can meet the new guidelines in order to obtain certification, as well as test assertions for how the accredited test laboratories will validate that the system complies with those requirements. The requirements and test assertions will be adjunct to the VVSG itself but will be subject to public review and comment, including distribution to the EAC's TGDC, Standards Board and Board of Advisors before implementation.

2.2. Scope

The Help America Vote Act (HAVA) of 2002, Section 301 (b) defines a voting system as "the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control and support the equipment that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information." This is the framework for all of the principles and guidelines, as well as the requirements and test assertions.

The scope of the VVSG 2.0 will continue to cover the ability to perform pre-voting, voting, and post-voting operations as confined within the framework set forth by the definition of a voting system in HAVA. The primary difference between the scope of VVSG 2.0 and that of the previous versions is that instead of creating guidelines based on voting devices; the scope of the VVSG 2.0 is focused on the core functions performed within a voting system. The 17 core functions identify the properties of an election that are agnostic to the technologies for implementing them. Those 17 Functions are:

1. Input Data for Ballot Construct
2. Associate Data for Ballot Construct
3. Ballot Layout

4. Ballot Generation
5. Ballot Transfer
6. Ballot Retrieval
7. Ballot Presentation
8. Capture Vote Selections
9. Interpret Vote Selections
10. Extract Vote Selections
11. Present Vote Selections
12. Transfer Vote Selections
13. Store Vote Selections
14. Retrieve Vote Selections
15. Tabulate Vote Selections
16. Transfer Results
17. Present Results

3.   Principle and Guidelines Overview

The principles and guidelines were designed to represent a logical framework, based upon the most stable, most timeless aspects of elections, which can provide a reliable basis for the more detailed processes of specification, implementation, and evaluation of election technology properties.

Voluntary Voting System Guidelines 2.0

Principles and Guidelines

Principle 1: HIGH QUALITY DESIGN
The voting system is designed to accurately, completely, and robustly carry out election processes.

> **1.1** - The voting system is designed using commonly-accepted election process specifications.

> **1.2** - The voting system is designed to function correctly under real-world operating conditions.

> **1.3** - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

Principle 2: HIGH QUALITY IMPLEMENTATION
The voting system is implemented using high quality best practices.

> **2.1** - The voting system and its software are implemented using trustworthy materials and best practices in software development.

> **2.2** - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers.

> **2.3** - Voting system logic is clear, meaningful, and well-structured.

> **2.4** - Voting system structure is modular, scalable, and robust.

> **2.5** – The voting system supports system processes and data with integrity.

> **2.6** - The voting system handles errors robustly and gracefully recovers from failure.

> **2.7** - The voting system performs reliably in anticipated physical environments.

Principle 3: TRANSPARENT
The voting system and voting processes are designed to provide transparency.

3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE
The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 – Standard, publicly-available formats for other types of data are used, where available.

4.3 – Widely-used hardware interfaces and communications protocols are used.

4.4 – Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS
All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 – Voters have a consistent experience throughout the voting process in all modes of voting.

5.2 – Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY
Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED
Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE
The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware and accessories protect users from harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 The voting system is evaluated for usability by election workers.

Principle 9: AUDITABLE
The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available 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.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY
The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Principle 11: ACCESS CONTROL
The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY
The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION
The voting system protects sensitive data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

Principle 14: SYSTEM INTEGRITY
The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

14.2 - The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING
The voting system provides mechanisms to detect anomalous or malicious behavior.

    15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

    15.2 - The voting system generates, stores, and reports all error messages as they occur.

    15.3 - The voting system employs mechanisms to protect against malware.

    15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.