**U.S. ELECTION ASSISTANCE COMMISSION**
633 3rd St. NW, Suite 200
Washington, DC 20001

# Voluntary Voting System Guidelines
# Version 2.0

# Test Assertions Version 1.4

Published: January 30, 2026

# Introduction

This document contains detailed test assertions for select *Voluntary Voting System Guidelines 2.0 Requirements* (*VVSG 2.0*). Test assertions were not developed for all VVSG 2.0 requirements. The requirements identified for test assertion development were flagged in several different ways, including:

- Public comment period of the DRAFT VVSG 2.0,
- Public hearings on the state of the DRAFT VVSG 2.0, and
- Internal review by EAC staff.

Many of the VVSG requirements focus on design at a high level and may be open to interpretation. In order to thoroughly test these requirements, manufacturers and voting system test laboratories (VSTL) need the ability to break down each VVSG requirement into unambiguous, specific, and testable conditions. Test assertions are a method to accomplish this. The test assertions contain granular conditions that must be tested to determine conformance to specific VVSG requirements. The overall goal of the assertions is to ensure that the VSTLs test each requirement in the VVSG correctly and comprehensively. EAC staff will regularly review and revise the test assertions with feedback from VSTLs, manufacturers, election officials, NIST, and other stakeholders and will make recommendations to the Executive Director for final approval. These test assertions help ensure uniformity and consistency among all the VSTLs and ensure the same pass/fail result regardless of which VSTL is used to test a specific voting system.

Test assertions are developed for a specific subset of VVSG 2.0 requirements. There are requirements identified as potentially ambiguous and/or difficult to test. Test assertions may ultimately be developed for more requirements in the VVSG. Upon using the test assertions during the EAC's Testing & Certification Program, issues may be identified that necessitate updates or completely new test assertions to be developed. Therefore, this effort is intended to be a living document that will be updated as needed.

# Organization and Structure of Test Assertions

The VVSG 2.0 test assertions are organized and numbered according to the principles and guidelines to which they are most applicable. Each assertion has the following fields:

- Number and title of each requirement
- Number of each test assertion
- Text of each test assertion and sub-assertion (Not all assertions will have sub-assertions)

Test assertions are indicated by the presence of the letters “TA” and followed by the original requirement number, a space, and a sequential number identifier. The original requirement number for each assertion is formatted consistently throughout this document according to the following legend:

$$\mathbf{TA}\underbrace{\mathbf{1.\,1.\,1-A}}_{w}\mathbf{.}\underbrace{\mathbf{1}}_{x}\mathbf{.}\underbrace{\boldsymbol{a}}_{y}\ \underbrace{\mathbf{1}}_{z}$$

$\boldsymbol{w}$ is the base requirement
$\boldsymbol{x}$ is the first numbered requirement or bullet under $\boldsymbol{w}$
$\boldsymbol{y}$ is the first lettered requirement under $\boldsymbol{x}$
$\boldsymbol{z}$ is the assertion sequential number identifier and is preceded by a space

# Technical terms used in the requirements

Unless otherwise specified, the intended sense of any technical terms is that which is commonly used by the information technology industry. In some cases, terminology is specific to elections or voting systems. Requirements that use words with special meanings are linked to their definitions in the VVSG 2.0 Glossary of Terms. Technical standards (e.g., ISO, ANSI) incorporated into the test assertions are fully cited in the VVSG 2.0, alongside other technical documents and references useful for understanding the information.

# Conformance Language

The text of a requirement is referred to as *normative*, meaning that the text constitutes the requirement and must be satisfied when implementing and testing the voting device or system. Text in this document that is not part of a requirement, such as the discussion field, is referred to as *informative*, meaning that it is for informational purposes only and does not contain requirements.

Test assertions are derived from the requirements and may also include additional information from the discussion fields. Assertions contain normative text and are designed to contain at least one keyword. Keywords are words that have a specific meaning within this document and are always capitalized. The following list of keywords is used within this document:

- **MUST:** indicates a mandatory requirement. Synonymous with "is required to."
- **MUST NOT:** also indicates a mandatory requirement, but the requirement is to not do something.
- **MAY:** indicates an optional, permissible action and often suggests one possible way of conforming to a more general requirement.

- **SHOULD:** indicates an optional action that is recommended, one that is particularly suitable, without mentioning or excluding others. When a requirement's discussion field indicates a preference for a particular action, that is an indicator that the "SHOULD" keyword is appropriate in the test assertions. Synonymous with "is permitted and recommended."
- **IF / THEN:** indicates a requirement contingent upon the existence of a feature or other condition.
- **EITHER**: indicates that there are alternate ways to fulfill a requirement.
- **ONLY:** indicates that an action can be performed solely in a single manner.

# Principle 1 – High Quality Design

## 1.1.2-F – Testing codes and image creation

**TA1.1.2-F 1**: Prior to opening the polls, the voting system MUST give election officials the capability to audit the encoded voter selections.

## 1.1.3-A – Opening the polls

**TA1.1.3-A 1**: Scanners and ballot marking devices MUST provide designated functions for entering voting mode.

**TA1.1.3-A 2:** Access control MUST be present to prevent the inadvertent or unauthorized activation of the poll-opening function.

**TA1.1.3-A 3:** Instructions for opening the polls MUST be provided on-screen.

**TA1.1.3-A 4:** Instructions for opening the polls MUST be provided in the TDP.

**TA1.1.3-A 5:** A means of verifying that the polls have been opened MUST be provided.

## 1.1.5-G – Record audit information

**TA1.1.5-G.2 1:** The geographical location of the device MAY include but not limited to: polling place name, address, or geographical coordinates.

**TA1.1.5-G.5 1:** Every sheet on a multi-sheet ballot MUST contain the sheet number as well as the ballot style ID.

## 1.1.6-C – Ballot separation when batch feeding

**TA1.1.6-C.3 1**: If the voting system marks the ballot, it MUST only be capable of marking outside of the bounds of the ballot selection area.

## 1.1.6-G – Scan to manufacturer specifications

**TA1.1.6-G 1:** The voting system MUST provide the mark detection threshold report to be available on an ad hoc basis to election officials.

## 1.1.6-I – Ignore extraneous marks inside voting targets

**TA1.1.6-I 1:** The voting system MUST NOT interpret imperfections in the ballot stock as valid marks as defined in the manufacturer's documentation.

**TA1.1.6-I 2:** The voting system MUST NOT interpret folds in the ballot stock as valid marks as defined in the manufacturer's documentation.

**TA1.1.6-I 3:** The voting system MUST NOT interpret insignificant marks identified within the voting target as valid marks as defined in the manufacturer's documentation.

## 1.1.6-J – Marginal marks, without bias

**TA1.1.6-J 1:** The voting system MUST NOT evaluate identical ambiguous marks as valid votes in one target area and as invalid votes in other target areas on the same ballot.

**TA1.1.6-J 2:** The voting system MUST evaluate identical valid marks made in identical marking positions on identical ballot pages as valid marks.

**TA1.1.6-J 3:** The voting system MUST evaluate identical invalid marks made in identical marking positions on identical ballot pages as invalid marks.

## 1.1.7-A – Exiting or suspending election mode

**TA1.1.7-A 1**: Scanners and ballot marking devices MUST provide designated functions for suspending voting mode.

**TA1.1.7-A 2:** Access control MUST be present to prevent the inadvertent or unauthorized activation of the poll-suspension function.

**TA1.1.7-A 3:** Instructions for suspending the polls MUST be provided on-screen, after beginning the suspension process.

**TA1.1.7-A 4:** Instructions for suspending the polls MUST be provided in the TDP.

**TA1.1.7-A 5:** A means of verifying that the polls have been suspended MUST be provided.

**TA1.1.7-A 6**: Scanners and ballot marking devices MUST provide designated functions for exiting voting mode.

**TA1.1.7-A 7:** Access control MUST be present to prevent the inadvertent or unauthorized activation of the poll-exiting function.

**TA1.1.7-A 8:** Instructions for exiting the polls MUST be provided on-screen, after beginning the exiting process.

**TA1.1.7-A 9:** Instructions for exiting the polls MUST be provided in the TDP.

**TA1.1.7-A 10:** A means of verifying that the polls have been exited MUST be provided.

## 1.1.8-B – Partisan primary elections

**TA1.1.8-B 1:** The voting system MUST be able to separately report the number of ballots read for all political parties in open primary elections.

**TA1.1.8-B 2:** The voting system MUST be able to separately report the number of ballots read for all political parties in closed primary elections.

**TA1.1.8-B 3:** The voting system MUST be able to separately report the number of ballots counted for all political parties in open primary elections.

**TA1.1.8-B 4:** The voting system MUST be able to separately report the number of ballots counted for all political parties in closed primary elections.

## 1.2-A – Assessment of accuracy

**TA1.2-A.1 1:** Voting systems interpreting human made marks MUST interpret valid marks created in accordance with the manufacturer's published specifications as valid marks.

**TA1.2-A.1 2:** Voting systems interpreting human made marks MUST NOT interpret invalid marks that do NOT meet the manufacturer's published specifications as valid marks.

## 1.2-E – Respond gracefully to stress of system limits

**TA1.2-E 1:** The voting system MUST alert the user that the system is nearing the limitations of the system.

## 1.2-H – Protect against failure of input and storage devices

**TA1.2-H 1:** The voting system MUST prevent the loss of voting data in the event of a data input failure without relying on re-casting ballots.

**TA1.2-H 2:** The voting system MUST prevent the loss of voting data in the event of a storage device failure without relying on re-casting ballots.

## 1.2-I – FCC Part 15 Class A and B Conformance

**TA1.2-I 1:** The voting system MUST comply with the Rules and Regulations of the Federal Communications Commission, Part 15; Class A or Class B requirements for radiated and conducted emissions by testing per ANSI C63.4-2014.

**TA1.2-I 2:** The voting system documentation MUST indicate whether devices comprising the system are intended to be located in non-polling places (Class A) or polling places (Class B).

## 1.2-J – Power supply from energy service provider

**TA1.2-J 1:** The polling place voting device MAY be powered by a 120/208 V three-phase system at a frequency of 60 Hz.

**TA1.2-J 2:** The single-phase power MAY be a leg of a 120/240 V single phase system.

# Principle 2 – High Quality Implementation

## 2.1-C – Acceptable coding conventions

**TA2.1-C 1:** The voting system manufacturer MUST declare a publicly available set of coding conventions.

**TA2.1-C 2:** The coding convention MUST appear in a publicly available book, magazine, journal, or on the Internet.

**TA2.1-C 3:** The voting system manufacturer MUST utilize a publicly available set of coding conventions for voting system software.

**TA2.1-C 4:** The coding convention MUST be credible.

**TA2.1-C 5:** The coding convention MUST be used by at least two organizations who are not voting system manufacturers.

**TA2.1-C 6**: IF there are exceptions to convention rules THEN the exceptions MUST be publicly available.

## 2.1-D – Records last at least 22 months

**TA2.1-D 1:** The manufacturer MUST document that the medium chosen for record retention is able to meet the required environmental parameters based on specifications of the chosen medium.

## 2.1.1-A – General build quality

**TA2.1.1-A.1 1:** Voting system manufacturers MUST document the quality assurance procedures used to ensure their products are free from damage or defects.

**TA2.1.1-A.2 1:** IF components from third-party suppliers are used within the voting system, THEN the voting system manufacturer MUST ensure that third-party suppliers document the quality assurance procedures used to ensure components supplied from third parties are free from damage or defect.

## 2.1.1-C – Durability of paper

**TA2.1.1-C 1:** The manufacturer MUST document the type of paper used by the voting system.

## 2.1.2-A – Electronic device maintainability

**TA2.1.2-A.1 1:** IF a voting system component is electronic THEN the voting system manufacturer MUST identify all test points in the voting system documentation.

**TA2.1.2-A.3 1:** IF a voting system component is electronic and IF a failure in the device occurs THEN physical or audible indicators related to that failure MUST be present.

**TA2.1.2-A.3 2:** IF a voting system component is electronic THEN the voting system manufacturer MUST identify the meaning of all physical or audible indicators related to failures in the voting system documentation.

## 2.1.2-B – System maintainability

**TA2.1.2-B.1 1:** Voting system documentation intended for election workers MUST specify methods that trained election workers, lacking a technical background, can use to detect routine and common voting system equipment failures.

**TA2.1.2-B.2 1:** The voting system MUST provide sufficient information to allow for a voting technician to diagnose a problem with the voting device.

**TA2.1.2-B.2 2:** Any alarms or other indicators used by the voting system MUST be sufficient to enable detection and diagnosis of components that require maintenance by a trained technician.

**TA2.1.2-B.3 1:** Field maintainable components MUST NOT require the use of proprietary tools to access or replace.

## 2.3-C – Separation of code and data

**TA2.3-C 1:** The voting system software MUST NOT compile instructions or logic from configuration files.

**TA2.3-C 2:** The voting system software MUST NOT interpret instructions or logic from configuration files.

**TA2.3-C 3:** The voting system software MUST NOT compile instructions or logic from any other source of data.

**TA2.3-C 4:** The voting system software MUST NOT interpret instructions or logic from any other source of data.

## 2.4-A – Modularity

**TA2.4-A 1:** The voting system software MUST have a singular purpose per module.

**TA2.4-A 2:** The voting system documentation MUST describe the design patterns used to achieve modularity in the application.

## 2.4-B – Module testability

**TA2.4-B 1:** The voting system software modules MUST be designed to be testable through the application of a test harness.

## 2.4-C – Module size and identification

**TA2.4-C 1:** The manufacturers declared coding conventions MUST specify a naming convention in order to ensure modules are easily identifiable.

## 2.5-B – Unsafe concurrency

**TA2.5-B 1:** The voting system manufacturer MUST provide documentation describing the means by which safe concurrency is ensured.

## 2.5.1-A – COTS compilers

**TA2.5.1-A 1:** Any COTS compiler used to compile the code MUST NOT be proprietary in nature.

## 2.5.1-C – Prevent tampering with code

**TA2.5.1-C 1:** The voting system manufacturer MUST provide documentation describing how they protect the code from tampering.

## 2.5.1-D – Prevent tampering with data

**TA2.5.1-D 1:** The voting system manufacturer MUST provide documentation describing how they protect the data, vote data, and audit records from tampering.

## 2.5.2-A – Input validation and error defense

**TA2.5.2-A 1:** Invalid inputs MUST NOT prevent a voting system from recovering from an error.

**TA2.5.2-A 2:** Recovery MAY be initiated by a system reboot.

**TA2.5.2-A 3:** Recovery MAY be initiated by an election worker.

## 2.5.4-M – Election integrity monitoring

**TA2.5.4-M 1:** Electronic devices MUST detect and prevent the accumulation of negative votes.

**TA2.5.4-M 2:** IF a negative vote is detected, THEN an election official MUST be alerted through audio and visual alert methods.

**TA2.5.4-M 3:** Electronic devices MUST detect and prevent the decrement of counters that record the number of ballots cast.

**TA2.5.4-M 4:** IF a counter is decremented, THEN an election official MUST be alerted through audio and visual alert methods.

**TA2.5.4-M 5:** Electronic devices MUST detect and prevent counters that record numbers of ballots cast that have a negative value.

**TA2.5.4-M 6:** IF a counter has a negative value, THEN an election official MUST be alerted through audio and visual alert methods.

**TA2.5.4-M 7:** Electronic devices MUST prevent the accumulation of more votes for a single candidate in a contest than the total number of ballots cast.

**TA2.5.4-M 8:** IF a candidate has more votes than ballots cast, THEN an election official MUST be alerted through audio and visual alert methods.

**TA2.5.4-M 9:** IF the voting system includes a ballot box, THEN it MUST have a method to allow election workers to visually verify that no ballots are present in the box prior to the polls opening.

## 2.6-B – No compromising voting or audit data

**TA2.6-B 1:** IF a recovery condition occurs due to an exception, THEN the voting system software MUST cryptographically validate the vote data following recovery from the exception.

**TA2.6-B 2:** IF a recovery condition occurs due to an exception, THEN the voting system software MUST cryptographically validate the audit data following recovery from the exception.

## 2.7-B – Continuous operation – typical environmental conditions

**TA2.7-B 1:** This requirement MAY be tested in tandem with 2.7-C and its test assertions. If tested in tandem with 2.7-C, upon the successful completion of the 2.7-C test assertions, this requirement will be satisfied.

## 2.7-C – Continuous operation – varied environmental conditions

**TA2.7-C 1:** The duration of these tests MUST be for 96 consecutive hours.

**TA2.7-C 2:** The voting system MUST be able to withstand continuous operational testing equivalent to MIL-STD-810-H, Method 502.7 Procedure II - Operation performed at a constant temperature of 50 degrees Fahrenheit for 24 hours.

**TA2.7-C 3:** The voting system MUST be able to withstand continuous operational testing equivalent to MIL-STD-810-H, Method 507.6 Procedure 1 – Natural Cycle B2, for 24 hours.

**TA2.7-C 4:** The voting system MUST be able to withstand continuous operational testing equivalent to MIL-STD-810-H, Method 507.6 Procedure 1 – Natural Cycle B1, for 24 hours.

**TA2.7-C 5:** Relative humidity MUST test the ranges of 25% to 80% for Natural Cycle B2 and 75% to 80% for Natural Cycle B1.

**TA2.7-C 6:** The voting system MUST be able to withstand continuous operational testing performed in normal environmental conditions, for 24 hours.

**TA2.7-C 7:** Continuous operation means exercising ballot-counting cycles, which vary by system type, for 15 minutes of each hour, and at the maximum rate calculated from the manufacturer's documented throughput rates.

**TA2.7-C 8:** The interval between reports MUST be no more than once per 4 hours of continuous operation.

## 2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating

**TA2.7-D 1:** Voting System devices that are intended to experience bench handling or bench maintenance MUST be able to withstand shock testing equivalent to MIL-STD-810H, Method 516.8, Procedure VI – Bench Handling.

## 2.7-E – Ability to support transport and storage physical environment conditions - non-operating

**TA2.7-E 1:** The voting system MUST be able to withstand vibration testing equivalent to MIL-STD-810H, Method 514.8, Procedure I – General Vibration, Transportation.

## 2.7-F – Ability to support storage temperatures in physical environment – non-operating

**TA2.7-F 1:** The voting system MUST be able to withstand high and low temperature storage testing equivalent to MIL-STD-810H, Methods 501.7 and 502.7, Procedure I-Storage.

**TA2.7-F 2:** Temperatures MUST test the ranges of -4 to +140 degrees Fahrenheit.

**TA2.7-F 3:** The voting system MUST be able to withstand uncontrolled humidity testing equivalent to MIL-STD-810H, Method 507.6, Procedure I-Natural Hot-Humid. Humidity MUST test the ranges of 25% to 80%.

**TA2.7-F 4:** The voting system MUST be able to withstand non-operational humidity expose per MIL-STD-810H, Method 507.6, Procedure I – Natural (Hot-Humid) for a minimum duration of 10 days or 10 x 24-hour cycles.

## 2.7-G – Electrical disturbances

**TA2.7-G 1:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-3 standard for radiated immunity test level 3 (10 V/m), without disruption of normal operation or loss of data.

## 2.7-H – Power outages, sags, and swells

**TA2.7-H 1:** The voting system MUST be capable of operating for a period of at least 2 hours on backup power, such that no voting data is lost, or corrupted and normal operations continue without interruption.

**TA2.7-H 2:** When backup power is exhausted the voting system MUST retain the contents of all memories intact.

## 2.7-I – Withstand conducted electrical disturbances

**TA2.7-I 1:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-4 standard for electrical fast transient protection, without disruption of normal operation or loss of data.

**TA2.7-I 2:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-5 standard for lightning surge protection**,** without disruption of normal operation or loss of data.

**TA2.7-I 3:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-11 standard for power dips, interruptions, and variations immunity, without disruption of normal operation or loss of data.

**TA2.7-I 4:** The voting system MUST NOT be disturbed by a temporary overvoltage of 120 % normal line voltage lasting from 3 ms to 0.5 s, applied in gradual steps of overvoltage across the line and neutral terminals.

**TA2.7-I 5:** The voting system MUST NOT be disturbed nor overheat for a permanent overvoltage of 10% above the nominal 120 V rating of the voting system, applied in gradual steps of overvoltage across the line and neutral terminals.

## 2.7-J – Emissions from other connected equipment

**TA2.7-J 1:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-6 standard for conducted immunity, without disruption of normal operation or loss of data.

## 2.7-K – Electrostatic discharge immunity

**TA2.7-K 1:** The voting system MUST be able to withstand testing in accordance with the latest IEC 61000-4-2, level 4, applying an air discharge or a contact discharge according to the nature of the enclosure of the voting system, and without damage, disruption of normal operation, or loss of data.

**TA2.7-K 2:** Application of electrostatic discharge points to COTS components MAY be performed.

**TA2.7-K 3:** The voting system may cycle power or have momentary interruption of power provided that normal operation is resumed without human intervention or loss of data.

# Principle 3 – Transparent

## 3.1.1-B – System overview, functional diagram

**TA3.1.1-B 1:** The system overview MUST include a functional diagram(s) of the voting system.

**TA3.1.1-B 2:** The functional diagram(s) MUST be at a system level.

**TA3.1.1-B 3:** The functional diagram(s) MUST depict all of the hardware platforms and software components developed by the vendor.

**TA3.1.1-B 4:** The functional diagram(s) MUST show how the components relate to each other, to include at a minimum data interchange.

**TA3.1.1-B 5:** The functional diagram(s) MUST show how the components interact, to include at a minimum all network communications.

## 3.1.1-E – Traceability of procured software

**TA3.1.1-E 1:** The documentation MUST contain a declaration of where the software was obtained.

**TA3.1.1-E 2:** If the open-source software packages are digitally signed by the author(s), then it MUST be tracked.

**TA3.1.1-E 3:** If the open-source software packages are not digitally signed by the author(s), then a hash MUST be provided by the manufacturer and confirmed by the lab.

## 3.1.2-B – Maximum tabulation rate

**TA3.1.2-B 1:** IF the voting system utilizes a bulk-fed scanner THEN the manufacturer documentation MUST specify the maximum tabulation rate for that scanner.

**TA3.1.2-B 2:** IF any individual component impacts the overall maximum tabulation rate, THEN the documentation MUST specify the tabulation rate for all such components.

**TA3.1.2-B 3:** IF any individual factor, such as paper size, impacts the overall maximum tabulation rate THEN the documentation MUST specify the tabulation rate for all such factors.

## 3.1.2-C – Reliably detectable marks

**TA3.1.2-C.1 1:** The voting system manufacturers MUST document what constitutes a valid mark.

**TA3.1.2-C.1 2:** Any system configurations or other settings that influence mark detection within that voting system (e.g., threshold settings) MUST be included in the documentation.

**TA3.1.2-C.2 1:** The voting system manufacturers MUST document marks that the voting system identifies as ambiguous.

**TA3.1.2-C.2 2:** IF ambiguous marks require adjudication, the voting system manufacturers MUST document the processes and procedures utilized for such adjudication.

**TA3.1.2-C.3 1:** The voting system manufacturer MUST document marks that do not constitute a valid mark.

## 3.1.3-A – System security documentation

**TA3.1.3-A 1:** The voting system security document MUST include a description of how election staff and election workers can leverage the security features provided by the voting system.

## 3.1.3-C – Physical security

**TA3.1.3-C 1:** The system security document MUST describe all physical security controls for each voting device.

**TA3.1.3-C 2:** Security controls MUST include procedural steps for election staff and workers to keep the voting system physically secure.

**TA3.1.3-C 3:** The system security document MUST describe the correct way to implement the physical security controls.

## 3.1.4-K – Open market procurement of COTS software

**TA3.1.4-K 1:** The installation documentation MUST identify where the COTS were procured.

**TA3.1.4-K 2:** Digital signatures for the COTS products MUST be provided.

## 3.1.4-M – Trusted storage media

**TA3.1.4-M 1:** The setup inspection process documentation MUST specify trusted storage media devices used to install voting system software or firmware onto the voting system.

**TA3.1.4-M 2:** Trusted storage media devices SHOULD be read-only storage devices.

**TA3.1.4-M 3:** Trusted storage media devices MUST be zeroed-out before first use.

**TA3.1.4-M 4:** Methods utilized for zeroization MAY include procedures listed in the latest version of *NIST SP 800-88: Guidelines for Media Sanitization*.

## 3.2-B – Minimum properties included in the setup inspection process

**TA3.2-B.2 1:** The setup inspection process documentation MUST include the process for checking digital storage locations.

**TA3.2-B.2 2:** IF there is an expected value, then that value MUST be documented.

**TA3.2-B.2 3:** The setup inspection process documentation MUST include the process for checking physical storage locations including but not limited to ballots, parts of an audit trail, etc.

**TA3.2-B.2 4:** IF physical storage locations are not intended to be empty before the polls open THEN the status and expected state of the physical storage locations MUST be specified in the setup inspection process documentation.

## 3.2-D – Installed software identification procedure

**TA3.2-D 1:** The setup inspection process documentation MUST include the procedures to identify that ONLY certified software is installed on programmed devices of the voting system.

## 3.2-E – Software integrity verification procedure

**TA3.2-E 1:** A cryptographic hash MUST be used to verify the integrity of software installed on programmed devices of the voting system.

**TA3.2-E 2**: The hash verification process MUST be able to be performed in a manner that is independent of proprietary manufacturer software and scripts.

**TA3.2-E 3:** The hash verification process MUST be able to be performed without requiring manufacturer assistance.

## 3.3-A – System security, system event logging

**TA3.3-A 1:** The manufacturer MUST supply documentation that is free of proprietary information, made publicly available, and containing the following information:

**TA3.3-A.1 1:** A description of event logging capabilities.

**TA3.3-A.2 1:** The purpose of the log (e.g., security, audit trail, I/O).

**TA3.3-A.2 2:** Details regarding the format of the log file.

## 3.3-B – Specification of common data format usage

**TA3.3-B 1:** For each voting system component and function, the manufacturer MUST supply documentation describing how the manufacturer has implemented the *NIST CDF* specifications.

**TA3.3-B 2:** The documentation provided by the manufacturer MUST be free of proprietary information and made publicly available.

## 3.3-C – Bar and other codes

**TA3.3-C 1:** The documentation MUST include the name and version of the standard used for barcodes or any codes used in the voting system.

**TA3.3-C 2:** The documentation MUST include how the data may be packed and compressed within the encoding process.

**TA3.3-C 3:** The barcode report MUST be detailed in a comprehensive manner to allow an auditor to decode and examine the content of the barcode.

# Principle 4 – Interoperable

## 4.1-C – Exchange of cast vote records (CVRs)

**TA4.1-C 1:** Devices that import CVRs SHOULD have the capability to import CVRs in the respective CDFs, in compliance with *NIST SP 1500-103 Cast Vote Records Common Data Format Specification*.

**TA4.1-C 2:** Devices that export CVRs SHOULD have the capability to export CVRs in the respective CDFs, in compliance with *NIST SP 1500-103 Cast Vote Records Common Data Format Specification*.

## 4.1-D – Exchange of voting device election event logs

**TA4.1-D 1:** The voting system MUST be capable of importing election event log data conforming to Election event logging common data format specification: *NIST SP 1500-101 Election Event Logging Common Data Format Specification.*

**TA4.1-D 2:** The voting system MUST be capable of exporting election event log data conforming to Election event logging common data format specification: *NIST SP 1500-101 Election Event Logging Common Data Format Specification.*

## 4.1-E – Voting device event code documentation

**TA4.1-E 1:** The manufacturer MUST provide a non-proprietary specification per device that contains the codes used in the device's election event log and the meaning of the codes.

**TA4.1-E 2:** The event codes SHOULD comply to the NIST SP 1500-101 schema for documentation of event codes.

## 4.1-F – Specification of common format usage

**TA4.1-F 1:** The specification MUST describe the implementation of the CDF specification sufficiently such that an auditor can independently interpret CDF files produced by the manufacturer.

**TA4.1-F 2:** The specification MUST describe the implementation of the CDF specification sufficiently such that an auditor can independently import CDF files into a manufacturer's device.

## 4.2-B – Public documented manufacturer formats

**TA4.2-B 1:** IF the voting system uses methods of compression outside the scope of the CDF, THEN these methods of compression MUST be publicly documented.

**TA4.2-B 2:** IF the voting system uses methods of encoding outside the scope of the CDF, THEN these methods of encoding MUST be publicly documented.

**TA4.2-B 3:** IF the voting system uses data formats outside the scope of the CDF, THEN these data formats MUST be publicly documented.

**TA4.2-B 4:** IF the voting system uses protocols outside the scope of the CDF, THEN these protocols MUST be publicly documented.

## 4.3-A – Standard device interfaces

**TA4.3-A 1:** IF the voting system uses peripherals, THEN the peripherals that connect to the voting system MUST use standardized hardware interfaces.

**TA4.3-A 2:** Standardized hardware interfaces MUST NOT require proprietary hardware.

**TA4.3-A 3:** Standardized hardware interfaces MUST NOT require the user to obtain licenses.

**TA4.3-A 4**: IF proprietary hardware or cabling is used to connect to voting system devices, THEN that hardware or cabling MUST terminate in a standard hardware interface.

**TA4.3-A 5:** IF proprietary hardware or cabling is used to connect to voting system devices, THEN that hardware or cabling MUST use a published communication protocol.

# Principle 5 – Equivalent and Consistent Voter Access

## 5.1-A – Voting methods and interaction modes

**TA5.1-A 1:** IF a voting system uses paper ballots, THEN the voting system MUST provide features that assist in the reading of such ballots.

**TA5.1-A 2:** IF a voting system uses paper verification, THEN the voting system MUST provide features that assist in the reading of such records.

**TA5.1-A 3:** IF a voting system uses paper ballots, THEN the voting machine MAY provide paper ballots in at least two font size ranges, 3.0mm to 4.0mm inclusive and 6.3 mm to 9.0 mm inclusive.

**TA5.1-A 4:** IF a voting system uses paper ballots, THEN the voting system MUST provide magnification of those records.

**TA5.1-A 5:** This magnification MUST be done using an electronic enhanced visual display.

**TA5.1-A 6:** This magnification MUST be compatible with the paper records' configuration.

**TA5.1-A 7:** The magnifier MUST provide legibility for the paper as actually presented on the system.

**TA5.1-A 8:** The manufacturer MAY provide the make and model number of readily available magnifiers that are compatible with the system.

**TA5.1-A 9:** The audio-tactile interface of the voting system MUST provide the same capabilities to vote as are provided by its visual interface.

**TA5.1-A 10:** The audio-tactile interface of the voting system MUST provide the same capabilities to cast a ballot as are provided by its visual interface.

**TA5.1-A 11:** IF a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, THEN the voting system audio-tactile interface MUST support voting a straight party ticket and then changing the choice in a single contest.

**TA5.1-A 12:** IF the voting system supports ballot activation the voting system MUST provide features that enable all voters to perform this activation.

**TA5.1-A 13**: One such feature MAY be smart cards providing tactile cues, so as to allow correct insertion.

**TA5.1-A 14**: One such feature MAY be smart cards providing audio cues, so as to allow correct insertion.

**TA5.1-A 15:** The voting system MUST provide features that enable all voters to independently cast their ballot.

**TA5.1-A 16:** The voting system MUST provide features that enable all voters to independently verify their vote.

**TA5.1-A 17:** The voting system MUST provide features that enable all voters to submit their ballots independently without manually handling the ballot or having another individual submit their ballot.

**TA5.1-A 18:** The voting system MUST provide features that enable all voters to submit their ballots privately without manually handling the ballot.

## 5.1-B – Languages

**TA5.1-B 1:** Both written and unwritten languages supported by the manufacturer MUST be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions, in both visual and audio formats where applicable.

## 5.2-A – No bias

**TA5.2-A 1:** For all contest choices on an audio ballot, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 2:** For all contest choices on an audio ballot, there MUST be no discernible differences in the audio presentation of the human speaker or synthetic voice.

**TA5.2-A 3:** For all contest choices on an audio ballot, there MUST be no discernible differences in the audio presentation of the voice characteristics including, but not limited to, speech rate, volume, and pitch.

**TA5.2-A 4:** For all ballot selections within a review screen on an audio ballot, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 5:** For all ballot selections within a review screen on an audio ballot, there MUST be no discernible differences in the audio presentation of the human speaker or synthetic voice.

**TA5.2-A 6:** For all ballot selections within a review screen on an audio ballot, there MUST be no discernible differences in the audio presentation of the voice characteristics including, but not limited to, speech rate, volume, and pitch.

**TA5.2-A 7:** For all undervotes within a review screen on an audio ballot, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 8:** For all overvotes within a review screen on an audio ballot, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 9:** For all audio voter verifiable audit records, presented separately from the review screen (e.g., readback of a VVPAT), there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 10:** For all audio voter verifiable audit records, there MUST be no discernible differences in the audio presentation of the human speaker or synthetic voice.

**TA5.2-A 11:** For all audio voter verifiable audit records, there MUST be no discernible differences in the audio presentation of the voice characteristics including, but not limited to, speech rate, volume, and pitch.

**TA5.2-A 12:** For all undervotes within an audio voter verifiable audit record, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 13:** For all overvotes within an audio voter verifiable audit record, there MUST be no discernible differences in audio presentation to the voter.

**TA5.2-A 14:** For all contest choices within the enhanced visual ballot mode (e.g., high contrast ballots), there MUST be no discernible differences in *visual* presentation to the voter.

**TA5.2-A 15:** For all contest choices on an enhanced visual ballot mode, there MUST be no discernible differences in the visual presentation of font properties including, but not limited to, family, style (bold, italic, underline), and size.

**TA5.2-A 16:** For all contest choices on an enhanced visual ballot mode, there MUST be no discernible differences in the visual presentation of text properties including, but not limited to, word and letter spacing, vertical and horizontal alignment, indentation, line height, and white space handling.

**TA5.2-A 17:** For all contest choices on an enhanced visual ballot mode, there MUST be no discernible differences in the visual presentation of color.

**TA5.2-A 18:** For all contest choices on an enhanced visual ballot mode, there MUST be no discernible differences in the visual presentation of background.

**TA5.2-A 19:** For all contest choices on an enhanced visual ballot mode, there MUST be no discernible differences in the visual presentation of margins, borders, padding, and spacing.

**TA5.2-A 20:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in visual presentation to the voter.

**TA5.2-A 21:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in the visual presentation of font properties including, but not limited to, family, style (bold, italic, underline), and size.

**TA5.2-A 22:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in the visual presentation of text properties including, but not limited to, word and letter spacing, vertical and horizontal alignment, indentation, line height, and white space handling.

**TA5.2-A 23:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in the visual presentation of color.

**TA5.2-A 24:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in the visual presentation of background.

**TA5.2-A 25:** For all ballot selections within a review screen on an enhanced visual ballot, there MUST be no discernible differences in the visual presentation of margins, borders, padding, and spacing.

**TA5.2-A 26:** For all undervotes within a review screen on an enhanced visual ballot, there MUST be no discernible differences in visual presentation to the voter.

**TA5.2-A 27:** For all ballot selections within an enhanced visual voter verifiable audit record presented separately from the review screen (e.g., readback of a VVPAT), there MUST be no discernible differences in visual presentation to the voter.

**TA5.2-A 28:** For all ballot selections within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in the visual presentation of font properties including, but not limited to, family, style (bold, italic, underline), and size.

**TA5.2-A 29:** For all ballot selections within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in the visual presentation of text properties including, but not limited to, word and letter spacing, vertical and horizontal alignment, indentation, line height, and white space handling.

**TA5.2-A 30:** For all ballot selections within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in the visual presentation of color.

**TA5.2-A 31:** For all ballot selections within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in the visual presentation of background (e.g., pattern, image).

**TA5.2-A 32:** For all ballot selections within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in the visual presentation of margins, borders, padding, and spacing.

**TA5.2-A 33:** For all undervotes within an enhanced visual voter verifiable audit record, there MUST be no discernible differences in visual presentation to the voter.

**TA5.2-A 34:** For all contest choices on a tactile ballot, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 35:** For all ballot selections within a review screen on a tactile ballot, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 36:** For all undervotes within a review screen on a tactile ballot, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 37:** For all overvotes within a review screen on a tactile ballot, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 38:** For all audio voter verifiable audit records, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 39:** For all undervotes within an audio voter verifiable audit record, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 40:** For all overvotes within an audio voter verifiable audit record, there MUST be no discernible differences in tactile presentation to the voter.

**TA5.2-A 41:** For all contest choices on a limited dexterity mode ballot (e.g., mouth stick, "sip and puff"), there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 42:** For all ballot selections within a review screen on a limited dexterity mode ballot, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 43:** For all undervotes within a review screen on a limited dexterity mode ballot, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 44:** For all overvotes within a review screen on a limited dexterity mode ballot, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 45:** For all audio voter verifiable audit records, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 46:** For all undervotes within a limited dexterity mode voter verifiable audit record, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

**TA5.2-A 47:** For all overvotes within a limited dexterity mode audio voter verifiable audit record, there MUST be no discernible differences in limited dexterity mode presentation to the voter.

## 5.2-C – Information in all modes

**TA5.2-C 1:** IF the voting system equipment used an interaction mode in accordance with *5.1-A - Voting methods and interaction modes*, THEN instructions to the voter MUST be presented in that same mode.

**TA5.2-C 2:** IF the voting system equipment used an interaction mode in accordance with *5.1-A - Voting methods and interaction modes*, THEN warnings to the voter MUST be presented in that same mode.

**TA5.2-C 3:** IF the voting system equipment used an interaction mode in accordance with *5.1-A - Voting methods and interaction modes*, THEN messages to the voter MUST be presented in that same mode.

**TA5.2-C 4:** IF the voting system equipment used an interaction mode in accordance with *5.1-A - Voting methods and interaction modes*, THEN notifications of undervotes or overvotes MUST be presented in that same mode.

**TA5.2-C 5:** IF the voting system equipment used an interaction mode in accordance with *5.1-A - Voting methods and interaction modes*, THEN contest options MUST be presented in that same mode.

## 5.2-D – Audio synchronized

**TA5.2-D 1:** The voting system MUST provide the option for synchronized audio output to convey the same information that is displayed visually to the voter, based on WCAG 2.0 and Section 508 guidelines.

**TA5.2-D 2:** If the ballot is hand-marked, and a write-in candidate has been voted for, then the voting system MUST convey that a write-in has been voted for, and MAY convey the content of the write-in vote.

**TA5.2-D 3:** The voting system MUST convey electronic write-ins to the voter exactly as they are entered.

## 5.2-E – Sound cues

**TA5.2-E.1 1:** IF the voting system provides sound cues as a method to alert the voter and the voting system is NOT in audio-only mode THEN the tone MUST be accompanied by a visual cue.

**TA5.2-E.1 2:** IF the voting system provides sound cues as a method to alert the voter and the voting system is in audio-only mode THEN the tone MUST NOT be accompanied by a visual cue.

**TA5.2-E.1 3:** IF the voting system beeps when the voter attempts to overvote THEN there MUST be an equivalent visual cue.

**TA5.2-E.2 1:** IF the voting system provides visual cues as a method to alert the voter and the voting system is NOT in visual-only mode THEN the visual cue MUST be accompanied by a sound cue.

**TA5.2-E.2 2:** IF the voting system provides visual cues as a method to alert the voter and the voting system is in visual-only mode THEN the visual cue MUST NOT be accompanied by a sound cue.

**TA5.2-E.2 3:** The equivalent visual cue MAY be the appearance of an icon.

**TA5.2-E.2 4:** The equivalent visual cue MAY be the appearance of a blinking element.

# Principle 6 – Voter Privacy

## 6.1-C – Enabling or disabling output

**TA6.1-C 1:** The voting system MUST allow the voter to independently disable the audio output resulting in a video-only presentation.

**TA6.1-C 2:** The voting system MUST allow the voter to independently disable the visual output resulting in an audio-only presentation.

**TA6.1-C 3:** IF the default audio output settings have been disabled during the voting session, THEN the voting system MUST allow the voter to independently re-enable the audio output.

**TA6.1-C 4**: IF the default visual output settings have been disabled during the voting session, THEN the voting system MUST allow the voter to independently re-enable the visual output.

**TA6.1-C 5**: IF the voter enables or disables the video or audio output THEN the voting system MUST notify the voter of the change by means of the output functionality that is enabled.

## 6.1-D – Audio privacy

**TA6.1-D 1:** IF the voting session is performed using an audio interface, THEN the auditory content and associated audio cues MUST NOT be discernible to any other individual in the polling place without the voter's consent.

**TA6.1-D 2:** IF headphones are used with an audio interface, THEN the headphones MUST have low sound leakage such that the auditory content and associated audio cues are not discernible to any other individual in the polling place without the voter's consent.

**TA6.1-D 3:** Low sound leakage for headphone use MAY be considered "efficient" if the audio content is indistinguishable to other individuals. This is defined as an average sound measurement of 30 - 40 dB at either the minimum distance between devices prescribed within manufacturer documentation, or four feet, at the default volume setting for a voting session.

**TA6.1-D 4:** IF ballot submission is performed using an audio interface, THEN the voting system MUST prevent any individual in the polling place (without the voter's consent) from perceiving any content on the ballot submitted by the voter during the voting session.

**TA6.1-D 5:** IF ballot submission is performed using an audio interface, THEN the voting system MUST prevent any other individual in the polling place (without the voter's consent) from perceiving any audible aspect of the input controls.

**TA6.1-D 6**: Input controls MAY include buttons, touchscreen input, "sip and puff", and other forms of interaction with the voting system.

## 6.2-A – Voter independence

**TA6.2-A 1:** Voting system features and attributes which support voter independence MUST follow the standards outlined in *Chapters 3 through 5 of Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines*.
The voting system MUST allow voters to independently mark their ballots.

**TA6.2-A 2:** The voting system MUST allow voters to independently mark their ballots.

**TA6.2-A 3:** The voting system MUST allow voters to independently verify their ballots.

**TA6.2-A 4:** The voting system MUST allow voters to independently cast their ballots.

**TA6.2-A 5:** In order to be accessible to individuals with disabilities, the voting system MUST ensure that these individuals have the same opportunity for access as for other voters.

**TA6.2-A 6:** In order to be accessible to individuals with disabilities, the voting system MUST ensure that these individuals have the same opportunity for participation as for other voters.

**TA6.2-A.1 1:** IF the voting system utilizes an end-to-end (E2E) architecture with paper receipts THEN E2E paper receipts MUST be accessible to individuals with disabilities.

# Principle 7 – Marked, Verified, and Cast as Intended

## 7.1-A – Reset to default settings

**TA7.1-A 1:** IF a voter changes any adjustable setting of the voter interface, during the voting session, THEN at the beginning of the next voting session, that setting MUST have the original default value.

**TA7.1-A 2:** IF a poll worker changes any adjustable setting of the voter interface, during the voting session, THEN at the beginning of the next voting session, that setting MUST have the original default value.

## 7.1-F – Using color

**TA7.1-F 1:** All information that uses color for emphasis, MUST be accompanied by some other non-color design element.

## 7.1-M – Audio comprehension

**TA7.1-M 1:** For both recorded and synthetic speech the audio presentation of verbal information MUST be readily comprehensible by voters who have hearing loss no greater than 25 db.

**TA7.1-M 2:** For both recorded and synthetic speech, the audio presentation of verbal information MUST be readily comprehensible by voters who are proficient in the language implemented and under test.

**TA7.1-M.1 1:** For both recorded and synthetic speech, candidate names MUST be capable of being pronounced as the candidate intends.

## 7.2-D – Scrolling

**TA7.2-D.2.a 1:** The fixed header or footer MAY contain the number of allowable candidates the voter is still capable of selecting.

## 7.2-H – Accidental activation

**TA7.2-H 1:** Voting system on-screen controls MUST prevent accidental activation.

**TA7.2-H 2:** Detecting accidental activation to a voter's touch MUST be included in the manufacturer's usability testing report per 8.3-A – Usability tests with voters.

**TA7.2-H 3:** Controls MUST NOT be placed in areas where users touch the device for support (e.g., device chassis, frame, screen bezel).

**TA7.2-H 4:** An on-screen navigational touch and lift motion MUST NOT result in the selection or deselection of any on-screen option (e.g., touch vote target scroll up and releasing should not activate any on-screen item).

**TA7.2-H 5:** An active, selectable area for a button MUST NOT extend outside the visual bounds of the button or control.

**TA7.2-H 6:** An active, selectable area for any touch area MUST NOT extend outside the visual bounds of the touch area or control.

**TA7.2-H 7:** Voting system physical controls MUST prevent accidental activation.

## 7.2-I – Touch area size

**TA7.2-I.1 1:** Touch targets MAY be smaller than 12.7 mm (0.5 inches) in vertical and horizontal dimensions for the purpose of touch screen calibration ONLY.

**TA7.2-I.2 1:** Touch targets MAY be closer than 2.54 mm (0.1 inches) for the purpose of touch screen calibration ONLY.

## 7.2-P – Floor space

**TA7.2-P 1:** For the floor area, intended for use by the voter, the voting system MUST be operable, when set up according to the documentation supplied by the manufacturer, on a floor space positioned for a forward approach or positioned for a parallel approach.

**TA7.2-P.2 1:** The voting system MUST allow adequate room for an assistant to the voter, when deployed according to the installation instructions.

**TA7.2-P.2 2:** Adequate room for the assistant MUST include clearance for entry to the voting station.

**TA7.2-P.2 3:** Adequate room for the assistant MUST include clearance for exit from the voting station.

## 7.2-R – Control labels visible

**TA7.2-R.1 1:** Labels on the voting system, used for control, necessary for the voter to operate the voting system, MUST be placed on a surface of the voting system where they are visible and legible to voters with normal eyesight (no worse than 20/40 corrected) from a seated posture.

**TA7.2-R.1 2:** Labels on the voting system, used for control, necessary for the voter to operate the voting system, MUST be placed on a surface of the voting system where they are visible and legible to voters with normal eyesight (no worse than 20/40 corrected) from a standing posture.

## 7.3-E – Feedback

**TA7.3-E 1:** After making a selection, a voting system MUST provide, to the voter, an unambiguous visual difference between selected choice(s) and the non-selected choices within a given contest.

**TA7.3-E 2:** IF the voting system uses a visual interface, THEN the voting system MAY indicate the selection of candidates and choices by the voter by displaying a checkmark beside the selected option.

**TA7.3-E 3:** IF the voting system uses a visual interface, THEN then the voting system MAY indicate the selection of candidates and choices by the voter by displaying an "X" beside the selected option.

**TA7.3-E 4:** IF the voting system uses a visual interface, THEN then the voting system MAY indicate the selection of candidates and choices by the voter by conspicuously changing its appearance.

**TA7.3-E 5:** IF the voting system uses a visual interface, THEN then the voting system MAY indicate the selection of candidates and choices by the voter by the use of highlighting around the chosen option.

**TA7.3-E 6:** IF a voting system implements an audio interface, THEN after making a selection, a voting system MUST provide, to the voter, an audio confirmation of the selected contest choice(s) within a given contest.

**TA7.3-E 7:** IF the voting system uses an audio interface, THEN then the voting system MAY provide a spoken confirmation after making a selection.

## 7.3-K – Warnings, alerts, and instructions

**TA7.3-K.1.a 1:** All warnings and alerts issued by the voting system MUST clearly state the nature of the problem, in plain language.

**TA7.3-K.1.b 1:** All warnings and alerts issued by the voting system MUST clearly state, in plain language, whether the voter has performed an invalid operation or whether the voter has attempted an invalid operation or whether the voting system has malfunctioned.

**TA7.3-K.1.b 2:** IF the voting equipment malfunctions, THEN a warning issued by the voting system related to this malfunction MUST include information pertaining to this malfunction.

**TA7.3-K.1.b 3:** IF the voter attempts an invalid operation, THEN a warning issued by the voting system related to this attempt MUST include information pertaining to this attempt.

**TA7.3-K.1.b 4:** IF the voter performs an invalid operation, THEN a warning issued by the voting system related to this performance MUST include information pertaining to this performance.

**TA7.3-K.1.c 1:** All warnings and alerts issued by the voting system MUST clearly state the responses available to the voter in plain language.

**TA7.3-K.2 1:** Each distinct instruction MUST be separated from all other instructions.

**TA7.3-K.2 2:** IF an alert is intended to confirm visual changes to the voter using an audio format, THEN the voting system MAY communicate this with a short text or sound.

**TA7.3-K.2.a 1:** IF the interface is a visual interface, THEN each distinct instruction MUST be separated spatially from other instructions.

**TA7.3-K.2.b 1:** IF the interface is an audio interface, THEN each distinct instruction MUST be separated from other instructions by a noticeable pause.

## 7.3-O – Instructions for election workers

**TA7.3-O 1:** In order to make instructions clear the instructions MUST conform to best practices for plain language.

**TA7.3-O 2:** In order to make messages clear the messages MUST conform to best practices for plain language.

## 7.3-P – Plain language

**TA7.3-P 1:** Instructional material for the voter that is inherent to the voting system MUST conform to best practices for plain language.

**TA7.3-P 2:** Instructional material for the voter that is generated by default MUST conform to best practices for plain language.

**TA7.3-P 3:** Instructional material for the election worker that is inherent to the voting system MUST conform to best practices for plain language.

**TA7.3-P 4:** Instructional material for the election worker that is generated by default MUST conform to best practices for plain language.

**TA7.3-P 5:** Best practices for plain language MAY include *Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers (Redish, Laskowski, NIST Interagency Report 7596, Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers, 2009).*

**TA7.3-P 6:** Best practices for plain language MAY include *https://www.plainlanguage.gov/*

**TA7.3-P 7:** IF an instruction is based on a limiting condition, THEN the condition SHOULD be stated first, and then the action to be performed SHOULD be stated after that.

**TA7.3-P 8:** The voting system SHOULD use familiar words.

**TA7.3-P 9:** The voting system SHOULD use common words.

**TA7.3-P 10:** The voting system SHOULD avoid technical or specialized words that voters are not likely to understand.

**TA7.3-P 11:** The voting system SHOULD issue instructions on the correct way to perform actions, rather than telling voters what not to do.

**TA7.3-P 12:** The system's instructions SHOULD address the voter directly rather than use passive voice constructions.

**TA7.3-P 13:** The voting system SHOULD avoid the use of gender-based pronouns.

# Principle 8 – Robust, Safe, Usable, and Accessible

## 8.1-H – Sanitized headphones

**TA8.1-H 1:** Headphones or handsets that can be sanitized MUST be provided as part of the voting system.

**TA8.1-H 2:** The voting system manufacturer MUST provide instructions on how to sanitize headphones or sanitize handsets.

**TA8.1-H 3:** The voting system manufacturer MUST provide a means to sanitize headphones or sanitize headsets.

**TA8.1-H 4:** The requirement for sanitized headphones or handsets MAY be achieved by providing single-use headphones.

**TA8.1-H 5:** The requirement for sanitized headphones or handsets MAY be achieved by providing sanitary coverings.

## 8.3-A – Usability tests with voters

**TA8.3-A 1:** The manufacturer MUST conduct realistic usability tests on the voting system.

**TA8.3-A 2:** The tests MUST include all voter activities in a voter session.

**TA8.3-A 3:** Voter activities MUST start with ballot activation.

**TA8.3-A 4:** Voter activities MUST end with verification and casting.

**TA8.3-A 5:** The usability tests MUST be performed upon a completely functioning product.

**TA8.3-A 6:** The test ballot used in the usability tests SHOULD look like a real ballot, such as the NIST test ballot.

**TA8.3-A 7:** The test ballot used in the usability tests SHOULD have at least twelve contests.

**TA8.3-A 8:** The test ballot used in the usability tests SHOULD have at least two ballot questions.

**TA8.3-A 9:** The test ballot used in the usability tests SHOULD have at least five propositions.

**TA8.3-A 10:** The test ballot used in the usability tests SHOULD have at least one multiple-vote contest.

**TA8.3-A 11:** The test ballot used in the usability tests SHOULD have at least one write-in contest.

**TA8.3-A 12:** The test script used in the usability tests, conducted by the manufacturer, MUST be realistic.

**TA8.3-A 13:** The test script MUST enable testing of all valid operations for the voter interface under test.

**TA8.3-A 14:** The testing environment for the usability tests, conducted by the manufacturer, MUST be realistic.

**TA8.3-A 15:** The testing environment MUST be set up as it would be in a polling place.

**TA8.3-A 16:** The usability tests conducted by the manufacturer MAY use the NIST medium complexity test ballot.

**TA8.3-A 17:** Manufacturers MAY define their own testing protocols for the usability tests.

**TA8.3-A.1 1:** Test participants MUST be representative of the general population.

**TA8.3-A.1 2:** The visual interface MUST be used.

**TA8.3-A.1 3:** The population under test MUST consist of a mix of voters including, but not limited to, users of different ages, genders, ethnicities, levels of education, voting experience.

**TA8.3-A.1 4:** The population under test MUST consist of voters who are eligible to vote in the U.S.

**TA8.3-A.1 5:** The population under test MUST NOT consist of voters who are, or have been, a poll worker, a voting machine manufacturer, a voting machine developer, in the marketing or sales of voting systems, or involved in any other position that is part of the voting process.

**TA8.3-A.1 6:** The population under test MUST NOT consist of voters who are involved with a usability or market research business/company.

**TA8.3-A.1 7:** The population under test SHOULD NOT consist of voters who have previously participated in a voting system usability test.

**TA8.3-A.1 8:** The manufacturer SHOULD ensure that at least 30 test participants are able to complete the testing session.

**TA8.3-A.1.a 1:** Each language supported by the voting system MUST have a test participant who speaks that language.

**TA8.3-A.1.a 2:** This test participant must speak the non-English language they are assigned to test as their primary language.

**TA8.3-A.1.b 1:** Test participants MUST include visually impaired voters using the audio format.

**TA8.3-A.1.b 2:** The visual acuity of these test participants MUST be less than 20/200 or these participants MUST NOT be able to use the low-vision interface.

**TA8.3-A.1.b 3:** Test participants MUST include visually impaired voters using tactile controls.

**TA8.3-A.1.b 4:** The manufacturer MUST ensure that at least eight visually impaired test participants are able to complete the testing session, without assistance.

**TA8.3-A.1.b 5:** The manufacturer SHOULD initially target at least 10 - 12 visually impaired participants, in order to ensure that at least eight visually impaired individuals are able to complete the testing sessions.

**TA8.3-A.1.c 1:** Test participants MUST include voters with low vision who use the enhanced visual interface with or without audio.

**TA8.3-A.1.c 2:** The usability tests MUST use individuals whose visual acuity is less than 20/70 but greater than or equal to 20/200.

**TA8.3-A.1.c 3:** The usability tests MUST use individuals who can only read large-print, high contrast text.

**TA8.3-A.1.c 4:** The summative usability tests MUST use individuals who are visually impaired. Wearing corrective lenses MUST NOT assist these individuals in reading normal sized text.

**TA8.3-A.1.c 5:** The manufacturer MUST ensure that at least eight individuals with low vision are able to complete the testing session, without assistance.

**TA8.3-A.1.c 6:** The manufacturer SHOULD initially target at least 10 - 12 individuals with low vision, in order to ensure that at least eight individuals with low vision individuals are able to complete the testing sessions.

**TA8.3-A.1.d 1:** Test participants MUST include voters with limited dexterity (e.g., inability to grip a pencil) who use the visual tactile interface.

**TA8.3-A.1.d 2:** The manufacturer MUST ensure that at least eight test participants with limited dexterity are able to complete the testing session, without assistance.

**TA8.3-A.1.d 3:** The manufacturer SHOULD initially target at least 10 - 12 participants with limited dexterity, in order to ensure that at least eight individuals with limited dexterity are able to complete the testing sessions.

**TA8.3-A.2 1:** The manufacturer MUST report the total number of participants tested and demographics of the participants.

**TA8.3-A.2 2:** Manufacturers SHOULD describe their recruiting strategy.

**TA8.3-A.2 3:** The manufacturer SHOULD detail any compensation given to participants.

**TA8.3-A.2 4:** The manufacturer MUST describe how the voters were screened and selected.

**TA8.3-A.2 5:** The manufacturer SHOULD note any differences between the users profiled as recruits and the users who participated in the actual study.

**TA8.3-A.2 6:** The manufacturer SHOULD include detailed tables of all participant demographics, whether or not they completed the test, as an appendix to the test report.

**TA8.3-A.2 7:** The manufacturer MUST report the test results for all participants, whether or not they completed the test, using the Common Industry Format modified for voting systems (CIF-for-Voting Systems).

**TA8.3-A.2 8:** The manufacturer SHOULD use the Modified CIF Template for manufacturers as a template and guidance for the semantics, content, and testing.

**TA8.3-A.2 9:** The manufacturer MUST ensure that the usability test report conforms to the formatting requirements of the Common Industry Format (CIF).

**TA8.3-A.2 10:** The manufacturer MUST ensure that the usability test report conforms to the content requirements of the Common Industry Format (CIF).

**TA8.3-A.2 11:** The usability test report MUST be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.

**TA8.3-A.2 12:** The Technical Data Package submitted to the EAC for national certification MUST contain the Usability Test Report.

**TA8.3-A.2 13:** The usability tests MUST measure metrics for efficiency, effectiveness, and satisfaction as defined in the ISO/CIF standard (ISO/IEC 25062:2006).

## 8.4-A – Usability tests with election workers

**TA8.4-A 1:** The documentation required for normal voting system operation MUST be presented at a level appropriate for election workers who are not experts in voting system and computer technology.

**TA8.4-A 2:** The documentation SHOULD NOT presuppose familiarity with personal computers.

**TA8.4-A 3:** Voting system polling, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to learn.

**TA8.4-A 4:** Voting system polling, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to understand.

**TA8.4-A 5:** Voting system polling, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to perform.

**TA8.4-A.1 1:** The usability tests MUST include voting system setup.

**TA8.4-A.1 2**: The usability tests MUST include opening the voting system.

**TA8.4-A.1 3:** The instructions MUST enable the election worker to verify that the voting system has been set up correctly (setup).

**TA8.4-A.1 4:** Voting system setup, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to learn.

**TA8.4-A.1 5:** Voting system setup, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to understand.

**TA8.4-A.1 6:** Voting system setup, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to perform.

**TA8.4-A.1 7:** The usability tests MUST include voting system polling.

**TA8.4-A.1.a 1:** The usability tests MUST include operation during voting.

**TA8.4-A.1.a 2:** The instructions MUST enable the election worker to verify that the voting system is in the correct working order to record votes (polling).

**TA8.4-A.1.b 1:** IF they are part of the voting system THEN the usability tests MUST include the use of assistive technology and/or language options.

**TA8.4-A.1.c 1:** The usability tests MUST include voting system shutdown.

**TA8.4-A.1.c 2:** IF it is supported by the voting system THEN the usability tests MUST include shutdown at the end of a voting day during a multi-day early voting period.

**TA8.4-A.1.c 3:** The instructions MUST enable the election worker to verify that the voting system has been shut down correctly (shutdown).

**TA8.4-A.1.c 4:** Voting system shutdown, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to learn.

**TA8.4-A.1.c 5:** Voting system shutdown, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to understand.

**TA8.4-A.1.c 6:** Voting system shutdown, as documented by the manufacturer, MUST be reasonably easy for the typical election worker to perform.

**TA8.4-A.1.d 1:** The usability tests MUST include shutdown at the end of voting including any reports.

**TA8.4-A.1.e 1**: The usability tests MUST include providing ballots in different languages.

**TA8.4-A.1.f 1**: The usability tests MUST include selecting the correct ballot type (e.g., for vote centers).

**TA8.4-A.1.g 1**: The usability tests MUST include setting up the voting system to use different interaction modes.

**TA8.4-A.2 1:** The manufacturer MUST conduct realistic usability tests on the voting system with representative election workers.

**TA8.4-A.2 2:** The test participants MUST include typical election workers and consist of a mix of workers including, but not limited to, workers of different ages, genders, ethnicities, levels of education, and voting experience.

**TA8.4-A.3 1:** The manufacturer MUST ensure that the election workers usability documentation/report is included in the TDP.

**TA8.4-A.3 2:** The election workers usability test report MUST be submitted to the EAC in the Common Industry Format modified for voting systems (CIF-for-Voting Systems).

**TA8.4-A.3 3:** The manufacturer MUST ensure that the usability test report conforms to the formatting requirements of the Common Industry Format (CIF).

**TA8.4-A.3 4:** The manufacturer MUST ensure that the usability test report conforms to the content requirements of the Common Industry Format.

**TA8.4-A.3 5:** The usability test report MUST be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.

**TA8.4-A.3 6:** The manufacturer usability report MUST contain all testing conducted by the manufacturer, from the previous test assertions.

# Principle 9 – Auditable

## 9.1.1-A – Software independent

**TA9.1.1-A 1:** An undetected fault or error in the voting system software or hardware MUST NOT lead to undetectable changes in election results.

**TA9.1.1-A.1 1:** IF a voting system is a paper-based system THEN it MUST generate a paper record of votes cast.

**TA9.1.1-A.1 2:** IF a voting system is an E2E system THEN it MUST produce cryptographic proof of the validity of cast votes as defined in section *9.1.6 – Evidence export*.

**TA9.1.1-A.2 1:** The voting system documentation must include a detailed description of how the voting system achieves software independence.

## 9.1.2-A – Tamper-evident records

**TA9.1.2-A 1:** Tamper-evident records produced by voting systems MUST enable detection of incorrect election outcomes. Such records may include, but are not limited to, paper records, CVRs, ballot images, and artifacts from a cryptographic E2E verifiable voting.

**TA9.1.2-A.1 1:** For each ballot cast by the voter, the voting system MUST capture the contents of each vote at the time the ballot is cast.

**TA9.1.2-A.1 2:** For each ballot cast by the voter, the voting system MUST EITHER capture the paper record for each vote at the time the ballot is cast, or the voting system MUST generate E2E artifacts for each vote at the time the ballot is cast.

**TA9.1.2-A.2 1:** All detected errors MUST be recorded in a manner that provides evidence of any attempted unauthorized modification or access to the record.

## 9.1.4-A – Auditor verification

**TA9.1.4-A 1:** The voting system MUST generate records that are easily accessible to an election official without the assistance from the voting system manufacturer or the use of additional software outside the scope of the certified voting system.

## 9.1.5-C – Paper record intelligibility

**TA9.1.5-C 1:** If the voting system presents non-human-readable ballot selections (e.g., barcodes or QR codes) THEN they MUST be accompanied by ballot selections presented in a human-readable format.

**TA9.1.5-C 2:** All human-readable text identifying recorded ballot selections MUST be presented using plain language.

## 9.1.5-G – Preserving software independence

**TA9.1.5-G 1:** The voting system MAY print a unique identifier on ballots.

**TA9.1.5-G 2:** The voting system MAY print the unique identifier in a different font style and/or color.

**TA9.1.5-G 3:** If the voting system prints a unique identifier on ballots, then it MUST only be capable of printing outside of any area containing voter selections.

**TA9.1.5-G 4**: The printing process SHOULD be preserved regardless of software or hardware updates.

## 9.1.6-E – Ballot receipt

**TA9.1.6-E 1:** The voting system MUST provide voters with a receipt that allows them to verify that their ballot selections were included in the reported election outcome.

**TA9.1.6-E 2:** Ballot receipts and their verification MUST conform to all applicable accessibility requirements in the VVSG.

**TA9.1.6-E 3:** Ballot receipts MUST conform to all applicable voter-privacy requirements in the VVSG.

## 9.1.6-G – Evidence export

**TA9.1.6-G 1:** Cryptographic evidence MUST NOT violate ballot secrecy.

**TA9.1.6-G.1 1:** Cryptographic E2E voting systems MUST be capable of exporting cryptographic evidence supporting the verification of ballot tabulation.

**TA9.1.6-G.2 1:** Cryptographic E2E voting systems MUST provide the cryptographic evidence in a non-proprietary and publicly available format.

## 9.1.6-H – Mandatory ballot availability

**TA9.1.6-H 1:** The voting system MUST provide evidence in such a manner that it may be published and made accessible to voters.

## 9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

**TA9.1.6-K 1:** The voting system records MUST NOT be generated in a proprietary format in order for auditors or observers to perform verification.

**TA9.1.6-K 2:** The voting system MUST NOT store records sequentially with identifiable information that could violate voter privacy; this includes but is not limited to date or time stamps, language preference, or methods of accessibility used.

## 9.4-A – Risk-limiting audit

**TA9.4-A 1:** IF a voting system uses a paper-based architecture, THEN the system MUST support an evidence-based election, which allows election officials to conduct a risk-limiting audit.

**TA9.4-A 2:** A voting system MAY be considered "efficient" IF it meets requirements *4.1-C - Exchange of cast vote records (CVRs), 9.4-C - Unique ballot identifiers, and 9.4-D - Multipage ballots*.

## 9.4-C – Unique ballot identifiers

**TA9.4-C 1:** The voting system MUST EITHER have the capability of preserving the ballot scanning order or MUST be capable of affixing a unique ballot identifier such as scanner ID, batch ID, or ballot card number.

## 9.4-D – Multipage ballots

**TA9.4-D 1:** The voting system MUST be capable of affixing a unique ballot identifier to each page of a multipage ballot as per 9.4-C - Unique ballot identifiers.

**TA9.4-D 2:** The voting system MUST specify the affixed page number or unique ballot card identifier for each record in the CVR report.

# Principle 10 – Ballot Secrecy

## 10.1-A – System use of voter information

**TA10.1-A 1:** The voting system MUST NOT have the capability to accept any identifying information about any voter.

**TA10.1-A 2:** The voting system MUST NOT have the capability to accept the first name of any voter.

**TA10.1-A 3:** The voting system MUST NOT have the capability to accept the last name of any voter.

**TA10.1-A 4:** The voting system MUST NOT have the capability to accept the address of any voter.

**TA10.1-A 5:** The voting system MUST NOT have the capability to accept information about the driver's license of any voter.

**TA10.1-A 6:** The voting system MUST NOT have the capability to accept the voter registration number of any voter.

**TA10.1-A 7:** The voting system MUST NOT have the capability to process any identifying information about any voter.

**TA10.1-A 8:** The voting system MUST NOT have the capability to process the first name of any voter.

**TA10.1-A 9:** The voting system MUST NOT have the capability to process the last name of any voter.

**TA10.1-A 10:** The voting system MUST NOT have the capability to process the address of any voter.

**TA10.1-A 11:** The voting system MUST NOT have the capability to process information about the driver's license of any voter.

**TA10.1-A 12:** The voting system MUST NOT have the capability to process the voter registration number of any voter.

**TA10.1-A 13:** The voting system MUST NOT have the ability to store any identifying information about any voter.

**TA10.1-A 14:** The voting system MUST NOT have the capability to store the first name of any voter.

**TA10.1-A 15:** The voting system MUST NOT have the capability to store the last name of any voter.

**TA10.1-A 16:** The voting system MUST NOT have the capability to store the address of any voter.

**TA10.1-A 17:** The voting system MUST NOT have the capability to store information about the driver's license of any voter.

**TA10.1-A 18:** The voting system MUST NOT have the capability to store the voter registration number of any voter.

**TA10.1-A 19:** The voting system MUST NOT have the ability to report any identifying information about any voter.

**TA10.1-A 20:** The voting system MUST NOT have the capability to report the first name of any voter.

**TA10.1-A 21:** The voting system MUST NOT have the capability to report the last name of any voter.

**TA10.1-A 22**: The voting system MUST NOT have the capability to report the address of any voter.

**TA10.1-A 23:** The voting system MUST NOT have the capability to report information about the driver's license of any voter.

**TA10.1-A 24:** The voting system MUST NOT have the capability to report the voter registration number of any voter.

## 10.2.1-B – Indirect voter associations

**TA10.2.1-B 1:** Indirect voter associations MUST be available only to authorized election personnel.

## 10.2.4-B – Logging of ballot selections

**TA10.2.4-B 1:** Ballot selections that have been made through adjudication MAY be captured in the audit trail.

# Principle 11 – Access Control

## 11.1-B – Voter information in log files

**TA11.1-B 1:** The voting system MUST NOT log the first name of any voter.

**TA11.1-B 2:** The voting system MUST NOT log the last name of any voter.

**TA11.1-B 3:** The voting system MUST NOT log the address of any voter.

**TA11.1-B 4:** The voting system MUST NOT log information about the driver's license of any voter.

**TA11.1-B 5:** The voting system MUST NOT log the voter registration number of any voter.

## 11.1-C – Preserving log integrity

**TA11.1-C.3 1:** The logs MUST NOT be capable of being deleted, except in the case of a complete system wipe and reinstallation procedure.

**TA11.1-C.3 2:** There MUST be functionality included in the system that allows exporting and archiving of all log data.

**TA11.1-C.3 3:** Log rotation MUST NOT be capable of deleting the logs. The logs MAY be saved or archived as a separate file but cannot be removed from the system.

# Principle 12 – Physical Security

## 12.1-A – Unauthorized physical access

**TA12.1-A 1:** The voting system MUST prevent access without intention.

**TA12.1-A 2:** The voting system MUST prevent opportunistic access, including, but not limited to, unauthorized access.

**TA12.1-A 3:** All unauthorized physical access attempts and successful events on the voting system MUST leave physical evidence.

**TA12.1-A 4:** IF unauthorized access occurs THEN the physical evidence MUST indicate the point of access.

**TA12.1-A 5:** All physical access points on the voting system MUST be capable of being secured by tamper prevention methods (e.g., locks) and tamper detection methods (e.g., seals, tape).

**TA12.1-A 6:** The voting system documentation MUST describe how to properly implement procedural and physical methods for detecting unauthorized access.

## 12.1-B – Unauthorized physical access alert

**TA12.1-B 1:** IF the voter-facing system component is in an activated stage and it is accessed in an unauthorized manner THEN the voter-facing system component MUST produce an alert.

**TA12.1-B 2:** Alerts produced by the voting system MUST be both audible and visual in nature.

**TA12.1-B 3:** Audible alerts produced by the voting system SHOULD be greater than 60 db.

**TA12.1-B 4:** Alerts MUST comply with requirements set forth in *7.3-K – Warnings, alerts, and instructions*.

## 12.1-C – Disconnecting a physical device

**TA12.1-C 1:** IF a voter-facing system component is in an activated stage and is physically disconnected THEN the voter-facing system component MUST produce an alert.

**TA12.1-C 2:** Alerts produced by the voting system MUST be both audible and visual in nature.

**TA12.1-C 3:** Audible alerts produced by the voting system SHOULD be greater than 60 db.

**TA12.1-C 4:** Alerts MUST comply with requirements set forth in *7.3-K – Warnings, alerts, and instructions*.

## 12.1-D – Logging of physical connections and disconnections

**TA12.1-D 1:** IF a voter-facing system component is in an activated stage and it is physically connected THEN the voter-facing system component MUST log the connection.

**TA12.1-D 2:** IF a voter-facing system component is in an activated stage it physically disconnected THEN the voter-facing system component MUST log the disconnection.

## 12.1-E – Secure containers

**TA12.1-E 1:** The manufacturer's documentation MUST specify tamper evident seals to be used for containers that store and transport voting system records (e.g., ballots).

**TA12.1-E 2:** The manufacturer's documentation MUST specify methods for properly applying seals on containers that store and transport voting system records (e.g., ballots).

**TA12.1-E 3:** IF unauthorized physical access to a container storing or transporting voting system records occurs THEN the tamper evident seals MUST leave evidence of tampering when installed as documented.

## 12.1-F – Secure locking systems

**TA12.1-F 1:** Documentation MUST be provided by the manufacturer for each key scheme supported.

## 12.1-G – Backup power for power-reliant countermeasures

**TA12.1-G 1:** IF the voting system employs a physical security mechanism that requires power to operate, THEN that physical countermeasure MUST continue to operate using backup power if the power fails.

**TA12.1-G.1 1:** IF a voting system employs a powered physical security countermeasure, switching from primary power to backup power supply MUST produce an alert.

**TA12.1-G.1 2:** Alerts produced by a powered physical countermeasure MUST be both audible and visual in nature.

**TA12.1-G.1 3:** Audible alerts SHOULD be greater than 60 db.

**TA12.1-G.1 4:** Alerts MUST comply with requirements set forth in *7.3-K – Warnings, alerts, and instructions*.

**TA12.1-G.2 1:** IF a power failure occurs for a physical security mechanism, THEN that physical countermeasure MUST automatically switch over to the backup power source.

**TA12.1-G.3 1:** IF the voting system employs a physical security mechanism that requires power to operate, THEN that physical countermeasure MUST generate an event log entry when it is switched to backup power.

## 12.2-A – Physical port and access least functionality

**TA12.2-A 1:** Any physical port or access point (e.g., panel, door) that is exposed MUST be essential to voting operations or testing the voting system or auditing the voting machine.

## 12.2-B – Physical port auto-disable

**TA12.2-B 1:** IF the voting system is in an activated state, THEN the voting system MUST automatically disable any digital communication port that is disconnected.

**TA12.2-B 2:** IF the voting system is in a suspended state, THEN the voting system MUST automatically disable any digital communication port that is disconnected.

# Principle 13 – Data Protection

## 13.1.2-A – Integrity protection for election records

**TA13.1.2-A 1:** The voting system MUST digitally sign CVRs when a ballot is cast.

**TA13.1.2-A 2:** The voting system MUST digitally sign a ballot image file when they are generated.

## 13.2-B – Verification of election records

**TA13.2-B.1 1**: IF any component of the voting system is receiving data from another component of the system, THEN it MUST validate the digital signature of the election data received.

**TA13.2-B.2 1**: IF a voting system is receiving election results, THEN it MUST log any verification error of received election results, as they occur, and present on-screen verification errors of the received election results, as they occur.

**TA13.2-B.4 1:** IF a voting system is receiving election results and IF the received election data fails verification, THEN it MUST NOT aggregate and MUST NOT tabulate any received election results.

## 13.3-A – Cryptographic module validation

**TA13.3-A.1 1**: Cryptographic modules used in the voting system MUST have an "Active" validation status on the NIST Cryptographic Module Validation Program (CMVP) website, at the time of certification.

## 13.4-A – Confidentiality and integrity protection of transmitted data

**TA13.4-A 1:** The receiving device MUST be cryptographically authenticated before a voting system device transmits information to another voting system device.

**TA13.4-A 2:** The originating device MUST be cryptographically authenticated before a voting system device transfers information to another voting system device.

**TA13.4-A 3:** The voting system must encrypt all data sent over a network.

**TA13.4-A 4:** IF a voting system is transmitting data, THEN it MUST verify EITHER the hash of all election data received via a network connection, or the digital signature of all election data received via a network connection before it is acted upon.

**TA13.4-A 5:** IF a voting system is transmitting data, THEN it MUST use ONLY FIPS-validated protocols for integrity protection over a network.

# Principle 14 – System Integrity

## 14.1-B – Addressing and accepting risk

**TA14.1-B 1:** The voting system manufacturer MUST document each risk in the risk assessment and describe either a technical control to mitigate the risk or document that the risk is accepted.

**TA14.1-B 2:** The voting system manufacturer MUST document the accepted risks and provide the reason that the risk is acceptable for the voting system integrity.

**TA14.1-B 3:** Voting system manufacturers SHOULD use the formats outlined in *NIST SP 800-31-1: Guide for Conducting Risk Assessments* or *ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management*.

## 14.2-A – Non-essential networking interfaces

**TA14.2-A 1:** The voting system manufacturer MUST document all essential features of the voting system.

**TA14.2-A 2:** The voting system manufacturer MUST disable all non-essential networking services as part of initial system configuration.

**TA14.2-A 3:** The voting system MUST disable all other non-essential features.

## 14.2-C – Wireless communication restrictions

**TA14.2-C 1:** The voting system MUST NOT establish wireless connections.

**TA14.2-C 2:** The voting system MUST NOT broadcast or advertise a wireless network.

**TA14.2-C 3:** The voting system MUST NOT accept connection requests.

**TA14.2-C 4:** The voting system MUST disable any wireless functionality by default.

**TA14.2-C 5:** Wireless device drivers MUST NOT be installed.

**TA14.2-C 6:** This MAY be accomplished via removing wireless hardware.

**TA14.2-C 7:** This MAY be accomplished via administrator-controlled device configurations.

**TA14.2-C 8:** This MAY be accomplished via disconnecting/unplugging wireless device antennas.

## 14.2-D – Wireless network status indicator

**TA14.2-D 1:** IF a voting system contains wireless functionality, THEN there MUST be a status indicator confirming that wireless networking functionality is disabled.

## 14.2-E – External network restrictions

**TA14.2-E 1:** IF a voting system can establish a connection to an external network, THEN the voting system MUST NOT allow any wireless or any wired connection to a network.

**TA14.2-E 2:** All voting system components MUST utilize non-routable IP addresses.

**TA14.2-E 3:** IF a voting system can establish a connection to an external network, THEN the voting system MUST NOT allow any device external to the voting system to connect to that network.

## 14.2-F – Secure configuration and hardening documentation

**TA14.2-F 1:** The manufacturer MUST provide a secure configuration document for all supported operating systems.

## 14.2-G – Unused code

**TA14.2-G 1:** The compiled voting system application MUST NOT contain unused and dead code.

## 14.2-H – Use of exploit mitigation technologies

**TA14.2-H 1:** The voting system platform MUST implement Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) or implement equivalent exploit mitigation technologies.

## 14.2-I – Importing software libraries

**TA14.2-I 1:** The voting system MUST NOT bulk import or include libraries that the voting application does not need to function.

## 14.2-J – Vulnerability management plan

**TA14.2-J 1:** The voting system manufacturer MUST specify a process for identifying vulnerabilities within the vulnerability management plan.

## 14.2-K – Known vulnerabilities

**TA14.2-K 1:** The voting system MUST NOT contain vulnerabilities listed in the National Vulnerability Database (https://nvd.nist.gov).

## 14.3-B – Criticality analysis

**TA14.3-B 1:** The voting system manufacturer MUST provide a written criticality analysis in the voting system documentation.

**TA14.3-B 2:** The criticality analysis MUST provide a model for identifying impact to security, privacy, and performance for failure or compromise.

**TA14.3-B 3:** The criticality analysis MUST identify critical components.

**TA14.3-B 4:** NISTIR 8179 and NISTIR 8272 MAY be used.

**TA14.3-B 5:** The criticality analysis MUST describe the process used to identify components as critical.

**TA14.3-B 6:** The criticality analysis MUST prioritize critical components.

**TA14.3-B 7:** The prioritization SHOULD be listed as low, medium, and high criticality.

**TA14.3-B 8:** The criticality analysis MUST NOT label all components with equal priority.

**TA14.3-B 9:** The voting system manufacturer MUST provide a written supplier impact analysis.

**TA14.3-B 10:** The voting system documentation MUST identify critical suppliers.

## 14.3.2-D – Integrity protection for software allowlists

**TA14.3.2-D 1:** The allowlist configuration file MUST be validated with a digital signature.

# Principle 15 – Detection and Monitoring

## 15.1-E – Configuration file access log

**TA15.1-E 1:** The voting system MUST log identifying information of EITHER the group accessing configuration files or identifying information of the role of users accessing configuration files.

**TA15.1-E 2:** The logged identifying information MAY include the username or the name of the user.

**TA15.1-E 3:** The voting system log MUST contain the time of access for a configuration file.

## 15.2-A – Presentation of voting application errors

**TA15.2-A 1:** IF an error occurs THEN the voting system application MUST provide user notification describing the application error in time for the user to react to it before performing other actions.

## 15.2-C – Logging system errors

**TA15.2-C 1:** System errors do not include errors made by the user, such as undervotes, overvotes, and blank ballots.

## 15.3-A – Malware protection mechanisms

**TA15.3-A 1:** IF a COTS workstation provides EMS functionality, THEN the voting system MUST utilize application allowlisting or MUST use digital signatures on the COTS EMS devices in order to protect against malware.

**TA15.3-A 2:** IF malware protection is an included feature of the system, THEN the voting system MUST launch applications providing malware protection before the voting application is loaded.

## 15.3-B – Updatable malware protection mechanisms

**TA15.3-B 1:** IF new malware signatures are received for COTS devices providing EMS functionality, THEN malware protection mechanisms MUST be capable of being updated with the new signatures.

## 15.3-D – Notification of malware detection

**TA15.3-D 1:** COTS workstations providing EMS functionality MUST immediately notify a user when malware is detected on COTS EMS devices.

**TA15.3-D 2:** COTS workstations providing EMS functionality MUST make malware detection notifications on-screen.

## 15.3-E – Logging malware detection

**TA15.3-E 1:** IF malware is detected THEN the voting system MUST log every instance of detection.

## 15.3-G – Logging malware remediation

**TA15.3-G 1:** The reimaging or reinstallation of the operating system MUST be logged and SHOULD be stored external to the voting system.

**TA15.3-G 2:** The malware detection logs SHOULD be downloaded and stored in a separate system prior to reimaging the system.

## 15.4-B – Secure network configuration documentation

**TA15.4-B 1:** The voting system documentation MUST include operating system configurations.

**TA15.4-B 2:** The voting system documentation MUST include database configurations.

**TA15.4-B 3:** The voting system documentation MUST include configurations for any other security relevant application or system.

**TA15.4-B 4:** IF a voting system provides networking connectivity, THEN it MUST provide best practices for system administrators and election workers.

## 15.4-C – Documentation for disabled wireless

**TA15.4-C 1:** The voting system documentation MUST include procedures to disable wireless functionality for all components of the voting system.

**TA15.4-C 2:** The voting system documentation MUST include instructions for physically removing power from any embedded wireless chipsets.

**TA15.4-C 3:** The voting system documentation MUST include instructions for physically disconnecting or removing antennas.

## 15.4-D – Rule and policy updates

**TA15.4-D 1:** The voting system MUST be capable of utilizing updated rules and policies for network appliances, to adjust to new capabilities.