Principle 3
TRANSPARENT

The voting system and voting processes are designed to provide transparency.

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

This section contains requirements on the content of the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, and "system" refers to a voting system or individual voting device. The user documentation is also included in the TDP given to test labs. The requirements are grouped as follows:

A. System Overview
B. System Performance
C. System Security
D. Software Installation
E. Setup Process
F. System Operations
G. System Maintenance
H. Training
I. CDF Specification

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation.

System Overview documentation explains the physical and logical structure of the system, its components, how it is structured, details about the software, and so forth. It is, essentially, an overview that helps the user to understand the system and that places subsequent more detailed documentation in this context.

3.1-A System overview

In the system overview, the manufacturer must provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

3.1-A.1 System overview, functional diagram

The system overview must include a high-level functional diagram of the voting system that includes all of its components. The diagram must portray how the various components relate and interact.

3.1-A.2 System overview, system description

The system description must include written descriptions, drawings and diagrams that present, as applicable:

1. a description of the functional components (or subsystems) as defined by the manufacturer (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships)
2. a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure
3. a concept of operations that explains each system function and how the function is achieved in the design
4. descriptions of the functional and physical interfaces between components
5. identification of all COTS products (both hardware and software) included in the system and/or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component
6. communications (dial-up, network) software
7. interfaces among internal components and interfaces with external systems
8. for components that interface with other components for which multiple products may be used, file specifications, data objects, or other means used for information exchange including the public standard used for such file specifications, data objects, or other means

9. benchmark directory listings for all software and firmware and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation

3.1-A.3 System overview, identify software and firmware by origin

The system overview must include the identification of all software and firmware items, indicating items that were:

1. written in-house
2. written by a subcontractor
3. procured as COTS
4. procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options

3.1-A.4 System overview, traceability of procured software

The system description must include a declaration that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

Discussion

For most noncommercial software, this would mean a declaration that the software was downloaded from the canonical site or a trustworthy mirror. It is generally accepted practice for the core contributors to major open-source software packages to digitally sign the distributions. Verifying these signatures provides greater assurance that the package has not been modified.

System Performance documentation gives details on how the system performs in normal operation and its constraints and limits.

3.1-B System performance

The manufacturer must provide system performance information including:

1. device capacities and limits that were stated in the implementation statement
2. if not already covered in the implementation statement, performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency
3. quality attributes such as reliability, maintainability, availability, usability, and portability
4. provisions for safety, security, privacy, and continuity of operation
5. design constraints, applicable standards, and compatibility requirements

3.1-B.1 System performance, maximum tabulation rate

The maximum tabulation rate for a bulk fed scanner must be documented by the manufacturer. This documentation must include the maximum tabulation rate for individual components that impact the overall maximum tabulation rate.

Discussion
The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.

3.1-B.2 System performance, reliably detectable marks

For an optical scanner, the manufacturer must document what constitutes a reliably detectable mark versus a marginal mark.

3.1-B.3 System performance, processing capabilities

The manufacturer must provide a listing of the system's functional processing capabilities, encompassing capabilities required by the VVSG, and any additional capabilities provided by the system, with a description of each capability.

1. The manufacturer must explain the capabilities of the system that were declared in the implementation statement.
2. Additional capabilities (extensions) must be clearly indicated.

3. Required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated.
4. Additional capabilities that function only when activated during installation or operation by the user must be clearly indicated.
5. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated.

System Security documentation describes the features of the system that provide or contribute to its security and includes how to operate the system securely. Physical security and audit are included in this documentation.

3.1-C System security

The manufacturer must provide information that enables the user to understand the security-related functions of the system and how they are to be used properly.

3.1-C.1 System security, access control implementation

Manufacturers must provide user documentation containing:

1. guidelines and usage instructions on implementing, configuring, and managing access control capabilities
2. an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system
3. an access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy
4. information on all privileged accounts included on the voting system

Discussion

Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementation of the voting system. The policies may be pre-defined within the voting system or provided as guidelines in the documentation. The access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy. Information on privileged accounts include the name of the account, purpose, capabilities and permissions, and how to disable the account in the user documentation.

3.1-C.2 System security, system event logging

Manufacturers must provide user documentation that:

1. describes system event logging capabilities and usage
2. publicly available and free of charge, fully documents the log format information

Discussion

The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent manufacturers to implement utilities to parse the log file. This documentation must be publicly available, free of charge, and not just in the TDP. The documentation may be housed by the EAC or the test lab.

3.1-C.3 Audit

The voting system's user documentation must fully specify a secure, transparent, workable and accurate process for producing all records necessary from the devices and carrying out audits.

Discussion

The voting system documentation needs to provide enough information for election officials to carry out all auditing steps. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit steps.

3.1-C.4 Physical security

Manufacturers must provide user documentation explaining the implementation of all physical security controls for the voting device, including model procedures necessary for effective use of countermeasures.

Software Installation documentation describes in exact detail what software is installed, how it is installed, and how it is to be maintained.

3.1-D Software installation

The manufacturer must provide a list of all software to be installed on the programmed devices of the voting system and installation software used to install the software in the user documentation.

Discussion
Software to be installed on programmed devices of the voting system includes executable code, configuration files, data files, and election specific software.

3.1-D.1 Software installation, software information

The manufacturer must provide at a minimum in the user documentation the following information for each piece of software to be installed or used to install software on programmed devices of the voting system:

1. software product name
2. software version number
3. software manufacturer name
4. software manufacturer contact information
5. type of software (application logic, border logic, third party logic, COTS software, or installation software)
6. list of software documentation
7. component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data)

3.1-D.2 Software installation, software location information

The manufacturer must provide in the user documentation the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the voting system.

Discussion
This requirement applies to software installed on programmed devices of the voting system. The full directory path is the final destination of the software when installed on non-volatile storage with a file system.

3.1-D.3 Software installation, election specific software identification

The manufacturer must identify election specific software in the user documentation.

3.1-D.4 Software installation, installation software and hardware

The manufacturer must provide a list of software and hardware required to install software on programmed devices of the voting system in the user documentation.

3.1-D.5 Software installation, software installation procedure

The manufacturer must document the software installation procedures used to install software on programmed devices of the voting system in user documentation.

3.1-D.6 Software installation, compiler installation prohibited

The software installation procedures used to install software on programmed devices of the voting system must result in no compilers being installed on the programmed device.

3.1-D.7 Software installation, programmed device configuration baseline binary image creation

To replicate programmed device configurations, the software installation procedures must create a baseline binary image of the initial programmed device configuration on an unalterable storage media with a digital signature.

3.1-D.8 Software installation, programmed device configuration replication

The software installation procedures must use the baseline binary image of the initial programmed device configuration on an unalterable storage media to replicate the configuration on to other programmed devices.

3.1-D.9 Software installation, software installation record creation

The software installation procedures must specify the creation of a software installation record that includes at a minimum:

1. a unique identifier (such as a serial number) for the record
2. a list of unique identifiers of unalterable storage media associated with the record
3. the time, date, and location of the software installation
4. names, affiliations, and signatures of all people present
5. copies of the procedures used to install the software on the programmed devices of the voting system

6. the certification number of the voting system
7. list of the software installed on programmed devices of the voting system
8. a unique identifier (such as a serial number) of the vote-capture device or EMS which the software is installed

3.1-D.10 Software installation, procurement of voting system software

The software installation procedures must specify that voting system software be obtained from test labs or distribution repositories.

Discussion
Distribution repositories provide software they receive to parties approved by the owner of the software.

3.1-D.11 Software installation, open market procurement of COTS software

The software installation procedures must specify that COTS software be obtained from the open market.

3.1-D.12 Software installation, erasable storage media preparation

The software installation procedures must specify how previously stored information on erasable storage media is removed before installing software on the media.

Discussion
The purpose of this requirement is to prepare erasable storage media for use by the programmed devices of the voting system. The requirement does not require the prevention of previously stored information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.

3.1-D.13 Software installation, installation media unalterable storage media

The software installation procedures must specify that unalterable storage media be used to install software on programmed devices of the voting system.

Setup Inspection documentation explains how to verify that the system is properly setup and configured, and how to monitor its operations.

3.1-E Setup inspection process

The manufacturer must specify a setup inspection process that the voting device was designed to support and description of the risks of deviating from the process in the user documentation.

Discussion
The setup inspection process provides a means to inspect various properties of voting devices as needed during the election process.

3.1-E.1 Setup inspection, minimum properties included in the setup inspection process

The setup inspection process must at a minimum include

1. the inspection of voting system software
2. storage locations that hold election information that changes during an election
3. other voting device properties
4. execution of logic and accuracy testing related to readiness of use in an election

3.1-E.2 Setup inspection, setup inspection record generation

The setup inspection process must describe the records that result from performing the setup inspection process.

3.1-E.3 Setup inspection, installed software identification procedure

The manufacturer must provide the procedures to identify all software installed on programmed devices of the voting system in the user documentation.

Discussion
This requirement provides the ability to identify if the proper software is installed and that no other software is present on programmed devices of the voting system. This requirement covers software stored on storage media with or without a file system.

3.1-E.4 Setup inspection, software integrity verification procedure

The manufacturer must describe the procedures to verify the integrity of software installed on programmed devices of voting system in the user documentation.

3.1-E.5 Setup inspection, election information value

The manufacturer must provide the values of voting device storage locations that hold election information that changes during the election, except for the values set to conduct a specific election in the user documentation.

3.1-E.6 Setup inspection, maximum and minimum values of election information storage locations

The manufacturer must provide the maximum and minimum values voting device storage locations that hold election information changes during an election can store in the user documentation.

3.1-E.7 Setup inspection, register and variable value inspection procedure

The manufacturer must provide the procedures to inspect the values of voting device storage locations that hold election information that changes for an election in the user documentation.

3.1-E.8 Setup inspection, backup power operational range

The manufacturers must provide the nominal operational range for the backup power sources of the voting device in the user documentation.

3.1-E.9 Setup inspection, backup power inspection procedure

The manufacturer must provide the procedures to inspect the remaining charge of the backup power sources of the voting device in the user documentation.

3.1-E.10 Setup inspection, cabling connectivity inspection procedure

The manufacturer must provide the procedures to inspect the connectivity of the cabling attached to the voting device in the user documentation.

3.1-E.11 Setup inspection, communications operational status inspection procedure

The manufacturer must provide the procedures to inspect the operational status of the communications capabilities of the voting device in the user documentation.

3.1-E.12 Setup inspection, communications on/off status inspection procedure

The manufacturer must provide the procedures to inspect the on/off status of the communications capabilities of the voting device in the user documentation.

3.1-E.13 Setup inspection, consumables quantity of voting equipment

The manufacturer must provide a list of consumables associated with the voting device, including estimated number of usages per quantity of consumable in the user documentation.

3.1-E.14 Setup inspection, consumable inspection procedure

The manufacturer must provide the procedures to inspect the remaining amount of each consumable of the voting device in the user documentation.

3.1-E.15 Setup inspection, calibration of voting device components

The manufacturer must provide:

1. a list of components associated with the voting device that require calibration
2. the nominal operating ranges for each component in the user documentation
3. the procedures to inspect the calibration of each component in the user documentation
4. the procedures to adjust the calibration of each component in the user documentation

3.1-E.16 Setup inspection, checklist of properties to be inspected

The manufacturer must provide a checklist of other properties of the voting device to be inspected, to include:

1. a description of the risks on not performing a given inspection in the user documentation
2. power sources
3. cabling, communications
4. capabilities
5. consumables
6. calibration of voting device components
7. general physical features of the voting device
8. securing external interfaces of the voting device not being used

System Operations documentation deals with operating and using the equipment to conduct elections, including for election setup, pre-election testing, voting operations, reporting, etc.

3.1-F System operations manual

The system operations manual must provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities, and central counting activities, as applicable, with regard to all system functions and operations.

Discussion

The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

3.1-F.1 System operations, support training

The system operations manual must contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, central election officials, election judges, and poll workers.

3.1-F.2 System operations, functions and modes

The manufacturer must provide a summary of system operating functions and modes to permit understanding of the system's capabilities and constraints.

3.1-F.3 System operations, roles

The roles of operating personnel must be identified and related to the operating modes of the system.

3.1-F.4 System operations, conditional actions

Decision criteria and conditional operator functions (such as error and failure recovery actions) must be described.

3.1-F.5 System operations, references

The manufacturer must also list all reference and supporting documents pertaining to the use of the system during election operations.

3.1-F.6 System operations, operational environment

The manufacturer must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including a statement of all requirements and restrictions regarding:

1. environmental protection

2. electrical service
3. recommended auxiliary power
4. telecommunications service
5. any other facility or resource required for the proper installation and operation of the system

3.1-F.7 System operations, readiness testing

The manufacturer must provide specifications for testing of system installation and readiness.

Discussion
Readiness testing refers to steps that election officials can take after configuring equipment to establish that it was correctly configured. Logic and accuracy testing would be part of this.

These specifications must cover testing of all components of the system and all locations of installation (e.g., polling place, central count facility), and must address all elements of system functionality and operations, general capabilities, and functions specific to particular voting activities.

3.1-F.8 System operations, features

The manufacturer must provide documentation of system operating features that includes:

1. detailed descriptions of all input, output, control, and display features accessible to the operator or voter
2. examples of simulated interactions to facilitate understanding of the system and its capabilities
3. sample data formats and output reports
4. illustration and description of all status indicators and information messages

3.1-F.9 System operations, operating procedures

The manufacturer must provide documentation of system operating procedures that:

1. provides a detailed description of procedures required to initiate, control, and verify proper system operation
2. provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)

3. provides procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state
4. defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system
5. defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. such information also must be provided for the interaction of the system with other data processing systems or data interchange protocols
6. provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail
7. supports successful ballot and program installation and control by central election officials
8. provides a schedule and steps for the software and ballot installation, including a table outlining the key dates, events and deliverables
9. specifies diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states

3.1-F.10 System operations, operations support

The manufacturer must provide documentation of system operating procedures that:

1. defines the procedures required to support system acquisition, installation, and readiness testing
2. describes procedures for providing technical support, system maintenance and correction of defects and for incorporating hardware upgrades and new software releases

3.1-F.11 System operations, transportation

The manufacturer must include any special instructions for the care and handling of voting devices and any removable media or records for

1. shipment
2. storage
3. archival

System Maintenance documentation deals with proper maintenance of the voting equipment and how to correct various issues or problems.

3.1-G System maintenance manual

The system maintenance manual must provide information to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field.

Discussion
Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

3.1-G.1 System maintenance, general contents

The manufacturer must describe service actions recommended to correct malfunctions or problems personnel and expertise required to repair and maintain the system, equipment, and materials facilities needed for proper maintenance.

3.1-G.2 System maintenance, maintenance viewpoint

The manufacturer must describe the structure and function of the hardware, firmware and software for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance and for identification of faulty hardware or software.

3.1-G.3 System maintenance, equipment overview details

The description must include a concept of operations that fully describes such items as:

1. electrical and mechanical functions of the equipment
2. how the processes of ballot handling and reading are performed (paper-based systems)
3. for electronic vote-capture devices, how vote selection and casting of the ballot are performed
4. how transmission of data over a network is performed (if applicable)
5. how data are handled in the processor and memory units
6. how data output is initiated and controlled
7. how power is converted or conditioned
8. how test and diagnostic information is acquired and used

3.1-G.4 System maintenance, maintenance procedures

The manufacturer must describe preventive and corrective maintenance procedures for hardware, firmware and software.

3.1-G.5 System maintenance, preventive maintenance procedures

The manufacturer must identify and describe:

1. all required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning
2. number and skill levels of personnel required for each task
3. parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance
4. any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for cots used in the system)

3.1-G.6 System maintenance, troubleshooting procedures

The manufacturer must provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

3.1-G.7 System maintenance, troubleshooting procedures details

The manufacturer must identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware and software. Descriptions must include:

1. steps to replace failed or deficient equipment
2. steps to correct deficiencies or faulty operations in software or firmware
3. modifications that are necessary to coordinate any modified or upgraded software or firmware with other modules
4. number and skill levels of personnel needed to accomplish each procedure
5. special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure
6. any coordination required with the manufacturer, or other party, for COTS

3.1-G.8 System maintenance, special equipment

The manufacturer must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

3.1-G.9 System maintenance, parts and materials

Manufacturers must provide detailed documentation of parts and materials needed to operate and maintain the system.

3.1-G.10 System maintenance, approved parts list

The manufacturer must provide a complete list of approved parts and materials needed for maintenance. This list must contain sufficient descriptive information to identify all parts by:

1. type
2. size
3. value or range
4. manufacturer's designation
5. individual quantities needed
6. sources from which they may be obtained

3.1-G.11 System maintenance, marking devices

The manufacturer must identify specific marking devices that, if used to make the prescribed form of mark, produce readable marked ballots so that the system meets the performance requirements for accuracy.

Discussion
Includes pens or pencils and possibly a compatible EBM.

3.1-G.12 System maintenance, approved manufacturers

For marking devices manufactured by multiple external sources, the manufacturer must specify a listing of sources and model numbers that satisfy these requirements.

3.1-G.13 System maintenance, ballot stock specification

The manufacturer must specify the required paper stock, weight, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of vote response fields and to identify unique ballot styles, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

3.1-G.14 System maintenance, ballot stock specification criteria

User documentation for optical scanners must include specifications for ballot materials to ensure that votes are read from only a single ballot at a time, without bleed-through or transferal of marks from one ballot to another.

3.1-G.15 System maintenance, printer paper specification

User documentation for voting systems that include printers must include specifications of the paper necessary to ensure correct operation, minimize jamming, and satisfy Requirement Part 1:6.4.4-B and Requirement Part 1:6.5.1-A.

Discussion

This requirement covers all printers, either stand-alone or integrated with another device, regardless whether they are used for reporting, for logging, for VVPR, etc.

3.1-G.16 System maintenance, maintenance environment

The manufacturer must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

3.1-G.17 System maintenance, maintenance support and spares

Manufacturers must specify:

1. recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation
2. recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation
3. organizational affiliation (e.g., jurisdiction, manufacturer) of qualified maintenance personnel

Training documentation lays out various information that would be important when training users on the voting equipment.

3.1-H Training manual

The manufacturer must describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

3.1-H.1 Training manual, personnel

The manufacturer must specify the number of personnel and skill levels required to perform each of the following functions:

1. pre-election or election preparation functions (e.g., entering an election, contest and candidate information designing a ballot generating pre-election reports)
2. system operations for voting system functions performed at the polling place
3. system operations for voting system functions performed at the central count facility
4. preventive maintenance tasks
5. diagnosis of faulty hardware, firmware, or software
6. corrective maintenance tasks
7. testing to verify the correction of problems

3.1-H.2 Training manual, user functions versus manufacturer functions

The manufacturer must distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.

3.1-H.3 Training manual, training requirements

The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, and poll workers.

Common data format documentation deals with all details of how a manufacturer implements a CDF.

3.1-I – Specification of common data format usage

Voting device and system manufacturers must include a freely-available specification describing how the manufacturer has implemented a NIST CDF specification for a particular device or function. This includes such items as:

1. descriptions of how elements and attributes are used
2. constraints on data elements
3. extensions as well as any constraints or extensions

Discussion

Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a NIST CDF specification for its voting devices and the types of data exchanged or exported.