Development Status and Supplemental Guidance for the VVSG 2007

March 29, 2006
John Wack
Software Diagnostics and Conformance Testing Division
NIST
Technical Guidelines Development Committee
March 29, 2006 Plenary Meeting

Outline

- Overview of VVSG volumes
- Overview of VVSG development
- Next steps
- Inclusion of Supplemental Guidance
Major VVSG Volumes

- Introduction
- Terminology Standard (Glossary)
- Product Standard
- Standard on Data to be Provided
- Testing Standard
Introduction

- Executive Summary
- Background
- Scope & Applicability
- Audience
- Description and rationale of significant changes vs. 2002 VSS or VVSG 2005
  - Document Structure
  - Precision and Testability
  - IV Systems Overview
  - Threat Analysis Overview
  - Auditing Assumptions
  - Coding Conventions
  - Logic Verification
  - Performance-based usability standards and testing
  - Public Information Package (PIP)
- Deletions
- Options not Standardized
- List of Sources Reviewed
Technical Guidelines Development Committee  
March 29, 2006 Plenary Meeting  

Product Standard  

- Conformance Clause  
- General Requirements  
  - General Design Requirements  
  - Security And System Integrity - Information Integrity, Media Protection, Physical Security, Contingency And Disaster Recovery, System Startup, Shut Down, and Deactivation, Cryptography, Access Control, System Integrity Management, Hardware Security, System Development and Maintenance  
  - Communications  
  - Accessibility, Usability, and Privacy  
  - H/W and S/W performance - Response Time, Printer etc., Reliability and Availability, Accuracy/Error Rates, Electrical/RF  
  - Workmanship - Engineering practices, General build quality, Durability, Safety, Security and Audit Architectural, Maintainability, Size, Space and Weight Issues, Temperature, Humidity and other Robustness  
  - Archival requirements - Archiving of Records, Archivalness of Media, Period of Retention  
  - Interoperability (Use of open standards, etc.)
Product Standard continued

• Requirements by Voting Activity
  – Election Programming
  – Ballot Preparation, Formatting, and Production
  – Equipment Preparation - Software Distribution, Software Installation
  – Polling Place Setup - Privacy Enclosures, General Access Requirements: Doors, Ramps, Signs, Lighting Etc.
  – Equipment Setup for Security and Integrity - Setup for Cryptographic IV System, Wireless On/off Type Issues, In Situ Logic and Accuracy Testing, Setup Validation
  – Opening Polls
    – Casting - Enabling Ballot, Ballot Presentation, Straight-party Voting, Spoiling, Etc., Accessibility/usability, Voting Session Privacy
  – Closing Polls
    – Counting - Performance, Error Rates, Usability for Election Officials
    – Reporting, Transmitting Results
    – Auditing and Independent Verification - VVPAT, Witness, End-End, etc.
Standard on Data to be Provided

- Technical Data Package
  - Scope
  - Implementation Statement
  - System Hardware Specification
  - Software Design and Specification
  - System Test and Verification Specification
  - Configuration Management Plan
  - Quality Assurance Program
  - System Change Notes
  - Configuration for Testing
Data to be Provided continued

- Voting Equipment User Documentation
  - System Overview
  - System Functionality Description
  - System Security Specification
  - System Operations Manual
  - System Maintenance Manual
  - Personnel Deployment and Training Requirements
- Certification Test Plan
- Public Information Package
- Data to be provided to Software Reference Library
Testing Standard

• Overview of Testing
• Introduction to Test Methods
  – Inspection
  – Functional Testing
  – Performance Testing (Benchmarking)
  – Security Penetration Testing
• Documentation and Design Reviews (Inspections)
  – Initial Review of Documentation
  – Physical Configuration Audit
  – Functional Configuration Audit
  – Examination of Vendor Practices for Configuration Management and Quality Assurance
  – Logic Verification
  – Source Code Review
  – Verification of Design Requirements in Product Standard
  – Security Review
  – Usability / Accessibility Review
Testing Standard continued

• Test Suite Overviews (high-level descriptions)
  – Hardware (Environmental, Shake and Bake, Emissions)
  – Usability (Performance-based Testing)
  – Counting & Reporting
  – Security (Similar to Error Case Tests)
  – Open-ended Functional Testing
  – Open-ended Security Testing
Who Will Use the VVSG?

- Besides testers and vendors, states, election officials, researchers, reviewers
- States and election officials need to know…
  - Does a system meet the VVSG requirements? If so, then
  - Do the requirements assume any procedures?
- Reviewers and researchers need to know…
  - How do requirements in combination with procedures satisfy threat models?
  - What other assumptions are made by the requirements?
  - What are the ramifications of using some voting systems on various requirements?
Supplemental Guidance

- All audiences benefit from knowing the context of certain requirements and any procedural assumptions made, or not made, by those requirements
- SG provides context for VVSG audiences on
  - what the functional requirements specify
  - what they omit
- NIST will include this Supplemental Guidance as appropriate in the VVSG 2007
Paper Spool Example

- VVPAT paper spools are permitted in VVSG 2005
- NIST would include SG recommending additional procedures to safeguard privacy
- Note: the VVSG 2005 requires an election management procedure for this case
Other examples

- NIST might include SG for
  - Brighter lights in polling place when small fonts on paper spools
  - More separation of certain voting systems to preserve privacy
  - Randomness of audits, announcements of audits
  - Clearing jams while opening up ballot box
  - Distribution of passwords or security information
Format

- NIST will include a section of SG, as needed, with each section of requirements
- SG could be in basic requirements form, with source of SG noted (e.g., VSS)
- Could be informative text with additional discussion
NIST will focus on building the VVSG Introduction
  - Overview of all volumes
  - Understandable to many audiences
  - Guide for remainder of VVSG

Continue to increase usability of TGDC site
Continue with research and coordination with election community
Include supplemental guidance in VVSG